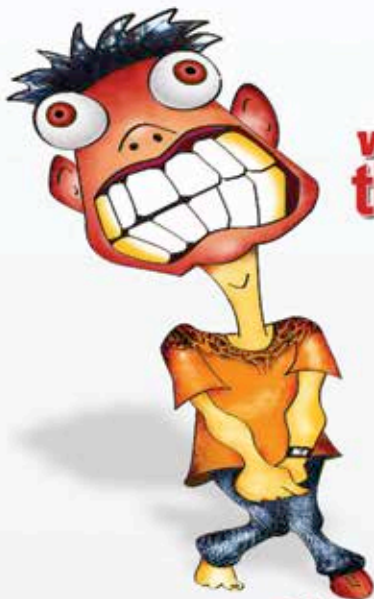


To CYBER CRIME

- What is Cybercrime?
- Various types of Cybercrime
- How to tell if you are a victim of crime
- Existing Indian laws pertaining to cybercrime, and how various crimes are treated
- Obscenity and slander, dos and don'ts and how you could break the law yourself unknowingly
- Cyber terrorism
- Safety tips for end users



**www.
thinkdigit/forum**

Join the forum to
express your views
and resolve your
differences in a more
civilised way.

**thinkdigit
FORUM**

Post your queries
and get instant
answers to all
your technology
related questions



One of the most active online technology forums
not only in India but world-wide

**JOIN
NOW**



www.thinkdigit.com



CYBER CRIME

powered by



CHAPTERS

CYBER CRIME

DECEMBER 2012

06

PAGE

What is Cyber Crime?

How is cyber crime actually defined and how does it affect our daily lives?

15

PAGE

The 12 Types of Cyber Crime

There are literally a dozen ways in which a cybercrime can be perpetrated, and you need to know what they are

36

PAGE

How to tell if you're a victim of cyber crime

Without you knowing it, you may be a victim of cybercrime. Here are simple things you can do to find out if you've been compromised

41

PAGE

Indian cybercrime laws

How is cybercrime policed in the Indian context and what laws govern Indian cyberspace

CREDITS

The people behind this book

EDITORIAL

Executive Editor

Robert Sovereign-Smith

Writers

Avinash Kothuri
Priyanka Mathur
Swapneel Rane
Tuba Raqshan
Vaibhav Kaushal

Features Editor

Siddharth Parwatay

Contributor

Copy: Infancia Cardozo

DESIGN

Sr. Creative Director

Jayan K Narayanan

Sr. Art Director

Anil VK

Associate Art Directors

Atul Deshmukh
Anil T

Sr. Visualisers

Manav Sachdev
Shokeen Saifi

Visualiser

Baiju NV

51
PAGE

Obscenity and slander: Don't break the law unknowingly

Simple things we do online may bring legal action your way. Read on and stay on the right side of the law

61
PAGE

Cyber terrorism

From your monitor to the valley of fear: Find out about the changing face of terrorism in the age of technology

79
PAGE

Cyber Warfare

Find out how the wars of the future are going to play out... In cyberspace

83
PAGE

Stay safe on the internet

Safety tips for end users in IT dealings. These simple things can keep you safe

© 9.9 Mediaworx Pvt. Ltd.

Published by 9.9 Mediaworx

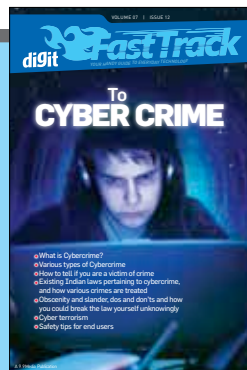
No part of this book may be reproduced, stored, or transmitted in any form or by any means without the prior written permission of the publisher.

December 2012

Free with Digit. If you have paid to buy this Fast Track from any source other than 9.9 Mediaworx Pvt. Ltd., please write to editor@thinkdigit.com with details

Custom publishing

If you want us to create a customised Fast Track for you in order to demystify technology for your community, employees or students contact editor@thinkdigit.com



COVER DESIGN: MIDHUN MOHAN


Introduction

Imagine a bespectacled shadowy figure sitting somewhere at an undisclosed location. Ordinarily, going by his attire or personality this person could be just your average Joe, but in this context he could be considered a suspicious and dangerous figure because of the context of what he is doing. He could be a cyber-stalker, a notorious hacker, or someone who is currently engaged in a coordinated cyber terrorism attack. Or perhaps (a comparatively lesser evil) he could be simply a mass mailer. In the course of performing all of these activities, he is for all practical purposes a cyber criminal.

This Fasttrack aims to introduce you to the technological transformation of crime from the streets to the networked superhighways of cyberspace. Driven by greed, revenge, obsession, megalomania, and even a righteous intent to protect national borders, cybercrime today has the potential to affect the lives of each and every one of us. Unlike ordinary criminals, this new breed of criminals needn't even be in your vicinity. For instance in the case of phishing, scam artists from another continent may prey on your greed and get you to part with your money.

In this Fasttrack we start off with defining what cybercrime is all about and acquaint you with the various types of tools cybercriminals use. Next we show you how to effectively monitor your PC and other devices for suspicious activity. But being affected at the personal level is not the only thing that cybercrime involves. There are wars of the digital era being fought in cyberspace. This comes under cyber terrorism and cyber warfare.

The laws relating to cybercrime are quite complex. Under the framework, simple things we unwittingly do online may be punishable and severe offenses may go unnoticed. Hence the need to know more about how cybercrime is policed in the Indian context and what laws govern Indian cyberspace.

We round up the Fasttrack with practical knowledge, and safety tips to keep yourself safe from being a victim of cybercrime. Happy reading and stay safe. 



WHAT IS CYBER CRIME?

How is cyber crime actually defined and how does it affect our daily lives?

Crime is that dark side of society that's too omnipresent to be overlooked. It's a bane to the harmony of society but it's hard to argue with the fact that humans, in general, tend to invest in activities where the returns are much higher than the effort needed to be put in and the risk of loss is much lower. The skill and expertise of a pickpocket or shoplifter is of no debate, and when a particular skillset enables someone to make a profit out of it, he is inclined to tap that resource no matter how morally dubious be the act. Over time, criminals have had to adapt new techniques and arm themselves with better equipment to keep up with ever changing technology.

Over the past two decades or so, computers and the internet have become an integral part of our everyday lives. People of all ages depend on digital technology, right from kids for games to teenagers who use it for educational and recreational activities like chatting, and adults who use it to make life much simpler and more productive. Almost every aspect of life has become digital, be it bank transactions or product purchase. It's high on accessibility, interactability and convenience. What's not to like? Unfortunately, this also makes it a hotspot for criminal activity. Because of the ease of access, and the potential damage that could be caused, cybercriminals are, in the modern world, perhaps the most dangerous type of criminals in existence. No wonder cyber crime has risen to the top priority for most governments to tackle, seeing how it's a constant threat to individuals, businesses and politics.

Defining Cyber Crime

So how exactly do we define “cyber crime”? Fundamentally any illegal activity committed using a computer and/or the internet can be called a cyber crime. Although the term is usually reserved for criminal activity wherein a computer or the internet is the location of the crime, it's also used to include traditional crimes in which computers or the internet are chief tools used in enabling the illegal activity. New technology in general creates new avenues for crime,

but not necessarily new types of crime. Criminals could commit fraud, thievery, identity theft, etc. even without the help of tech. These atrocities existed long before the word “cyber” came along. Thus, cyber



crime is basically an extension of existing criminal activity, perhaps making it easier while also adding new dimensions to its execution. Broadly put, cyber crime could be defined as “an illegal act where a computer or a computer network serves as the location, means, target or source of the act”. Legally also, this definition of cyber crime was agreed upon by most of the

European and North American countries at the Budapest Convention on Cybercrime that entered into force on July 1st, 2004.

When cyber crime took its roots

Since the beginning of the computer age, scientists and programmers have been working to find vulnerabilities in software and hardware products. When computer technology was relatively new, and networks were first gaining prominence in the 1990s, those who engaged in illegal hacking activities only did so to improve their knowledge of the systems that they were using, so that they could pit themselves against other competitors and be heralded as the better hacker. Thus, any highly dangerous activity such as intrusions into military installations or commercial organizations was perhaps nothing more than a nuisance. Since they weren't done with the intention of gaining profit, they didn't pose a long-term threat to security or raise concern to the level normally associated with criminal behaviour. Yet, as history pays testament, when people develop skills that give them some sort of an advantage over society, some of them will eventually use it to try to exploit and victimize society with their skill set. Enterprising criminals, aided by the massive growth in computer ownership and the financial transactions that take place throughout the internet, learned to exploit the vulnerabilities to commit cyber crime. This new breed of cybercriminal is no longer motivated solely by ego and tech ability. Cybercriminals have slowly discovered that the skills that they learnt as teens could now be used to make a comfortable living for themselves.

The effects of cyber crime on society

Studies show that on an average, more than one cyber crime occurs every 10 seconds. If that hit rate is not alarming enough, the fact that absolutely everyone is equally vulnerable to getting hit makes it worse. There have been recorded losses of over \$500 million in one year solely due to cyber crime. The need for drastic measures against cyber crime would become extremely clear once we observe the effects of cyber crime.

The crime is, basically, an attack on information about people or groups, and though the attack isn't physical (it's virtual), it's equally harmful. In a day and age where our virtual identities are just as important as our real identities, cyber criminals are mindful of the fact that all our personal information is centralised and we – the common man, our businesses, governments and properties – are extremely reliant on computers. Let's

look at how each of these four important parts of our lives are turned upside down by cyber crime.

- ▶ **Cyber crime against people:** This includes a wide variety of offenses. Criminals will hide behind fake promotions, offers, giveaways etc. while giving you the illusion of security to get you to give up your personal information. Impersonating institutions such as banks, they gain access to your info by convincing you that there's a problem with your account details and thereby ask you to 'rectify' it. Schemes such as the Nigerian letter scam or the chain-letter scams that were once practised via snail mail have now gone digital. Internet auction fraud is another way of duping people with non-delivery of product or misuse of credit card information. The trafficking of sexually explicit material including child pornography, which is illegal, is another major offense. Cyber defamation is committed when libellous claims about another individual are posted on a website or sent through an email. Social networks and chat services are not bereft of its presence. Online harassment or cyber bullying is a pretty common occurrence on such services. Yet another type of unwelcome engagement is cyber stalking –having your every action online followed



Criminals impersonate sites to get your sensitive information

- as and when it happens. In some of the more serious cases, the internet is used as a medium to locate individuals, engage them in conversation, invite them over for a personal meeting and then once the perpetrators meet the victim commit serious crimes such as rape, theft, murder etc.
- ▶ **Cyber crime against property:** basically involves the infiltration of computers with malicious software through websites, email or personal chats. These malware attacks could be just to destroy someone's computer or to steal information from them. These attacks deny the user access to his/her information while supplying the perpetrators with essential details about the victim. Theft of bandwidth, that is gaining unauthorized access to an internet connection, is also treated as a cyber crime.
- ▶ **Cyber crime against businesses:** These happen when the perpetrators

hack into the systems of the companies in question. Most businesses store their sensitive information on servers and the data may or may not be financial in nature. Hackers who can gain access into the systems of these companies get access to all the information available in these files. They can choose to destroy or leak them, or where money is concerned transfer funds from an organization to someone else's account. That's not the only downside to being hacked. The customers of that particular company lose faith in the organization such cases and thus, businesses



Hackers can operate from anywhere

can lose a significant number of customers based on incidents such as these. Also, the time spent by the IT professionals of the companies in trying to avoid these situations could instead be used for more productive purposes. Thus, even the threat of cyber crime can result in lower pro-

ductivity levels. When a business's website is hacked, it tends to lose traffic which translates into loss of revenue for the unfortunate company.

- ▶ **Cyber crime against governments:** Cyber criminals can attack organizations of any kind and government organizations are not an exception. The secure database of a government agency can be hacked with the intention to misuse sensitive information and the term “cyber-terrorism” is often used in this context. The term is defined by the FBI as “the pre-meditated, politically motivated attack against information, computer systems, computer programs and data which results in violence against non-combatant targets by sub-national groups or clandestine agents”. Basically, any individual or group gaining access to any sensitive information pertaining to the government and using it to cause disharmony, are cyber-terrorists. Strong political agenda might also be behind these cyber attacks against the government. Cyber crime could be used to undermine the effectiveness of a government, thus reducing the faith of citizens in a particular government.

Another form of cyber attack against the government is “hacktivism”. It is a somewhat recent development, and is basically activism in the cyber

world where activists protest or target information of the group they're protesting against. They gain access to government or private databases to obtain confidential information that could be used against the corporation. They could also disrupt the functioning of a site or shut it down completely as a form of protest. Though hacktivists don't commit cyber crime for personal/monetary gain, it still affects the privacy of a group of people and poses a risk to virtually stored information.

Cyber crime is easy

Considering the number of ways by which perpetrators can affect our lives using the internet, it's no puzzle to see why they're doing it. It's easy. Other than just the profitable nature of committing crimes online, there are many more reasons why the internet is a hot bed of criminal activity for most. Firstly, heavy initial investment is not needed. In petty, traditional crimes such as mugging, the perpetrators are required to have the basic know-how and/or weapons with them. For a more complex crime such as robbing a bank, the criminals are required to have a network of allies and equipment along with them to successfully execute the plan. This, of course, requires a lot of planning and finances. On the other hand, for a hacker to gain access to your account details or finances, access to a computer and technical know-how is all that is required. There's also the additional risk of retaliation from the victim or the chance of being caught in the act, which is much higher in the physical world. This could result in injury and legal action against the perpetrator. Online though, the evil techie could easily operate from a remote location where law enforcement doesn't pose so much of a risk. For him, it's a global playground where there's less risk of being caught while playing dirty. Through the very systems that run e-commerce, they are easily able to commit crimes. Thus, the entry into the cybercriminal world is much easier than in the real world. Add to the fact that on the internet there's not much competition or rivalry that exists in the real world. Infact, groups of online infiltrators often collaborate to improve their skills and seek out new opportunities, unlike real world gangs who fight for control. The icing on the cake is the advantage of



anonymity. Their identity in the virtual world remains there. In addition, any number of virtual identities are possible and they can operate their criminal activities using any of these virtual identities. This makes the task of identifying the perps extremely difficult for the victims and the investigators.

Significance of cyber crime

Cyber crime has a tremendous impact on the victims and on the judiciary system in general. Since it can easily go undetected and unreported, it's very tough to measure the magnitude of the resulting problems. The number of threats has only increased by leaps and bounds ever since the start of the 21st century. According to recent surveys, the frequency of successful cyber attacks has more than doubled over the past three years, and around 60-65% of citizens worldwide have already been affected by some form of cyber crime. The vast majority of these cases contain elements of fraud and involve financial loss by the victim. The most common targets of cyber criminal activity are found to be government offices and financial institutions. It's a load off our chest though knowing that according to psychologists, the majority of teenage hackers are doing it for the motive of recreation rather than for profit or causing harm.

The aspect of cyber crime that makes it extremely convenient and dangerous is its non-local character – The perpetrator and the victim of the same crime could be separated by a vast distance. This poses several problems when it comes to law enforcement, as the legal implications of the crime could vary in each country. As an example, take the hypothetical case of a person accessing child pornography located on a computer in a country that doesn't ban it. It becomes difficult to determine whether or not he's committing a crime. The problem lies in the undefined location of the source of the crime. The internet offers multiple hiding places in the network and also in the real world. However, cybercriminals leave clues about their identity and location, despite their best efforts to cover their tracks. But, in order to be able to follow up on such clues across national boundaries, there must be treaties of some sort regarding cyber crime between different countries, as the jurisdictions applying to each might differ.

Counter-measures by nations of the world

In 1996, the Council of Europe, together with representatives from the states of Canada, Japan and the United States drafted a preliminary international treaty covering computer crime. There was some rebellion to this though,

as the civil libertarian groups didn't approve of the provisions in the treaty which required internet service providers to store customer transactions and be able to turn them over on demand. However, work on the treaty proceeded. This led to the International Convention on Cybercrime in Budapest in 2001, which was signed by thirty countries, including Japan, South Africa, Canada and the US. The convention agreement authorizes a global cyber police force to investigate cyber crime. This meant that investigators had the power to track down network communications and to store intercepted data across countries. For this to work, nations must cooperate with each other by sharing gathered information and evidence related to cyber crime. Additional protocols covering terrorist activities and racist and xenophobic cyber crimes were proposed in 2002. The convention didn't necessarily guarantee that the issue of cyber



Lots of Antivirus softwares to choose from


crime would have an immediate solution. The provisions could come into full effect only if they were approved by that country's national legislature.

Despite all of the controversy surrounding the convention and the surveillance powers given to the nations who adopt it, the treaty is still a step ahead in the capturing and prosecution of cyber criminals. Since then, a plethora of laws have been adopted across the different countries of the world reinforcing them against the threat of cyber crime. Illegal or unauthorized use of a computer system, theft of private data and digital fraud are considered acts of felony in the US. Organizations without a viable network security program can be held responsible for negligence in the event of a cyber attack. Similarly, India has taken up legal actions to fight the menace, which will be discussed in a later chapter in this book.

The best defence is the best defence

Despite network security programs and organizations working to counteract cyber threats, cyber crime trends continue. Thus, it's best for us, the average computer user, to equip ourselves with the right equipment to protect our-

selves from being cheated online. Anybody who uses the internet is at risk of becoming a victim. Vulnerability to these attacks makes it much easier for the perpetrator. There are organizations like McAfee and Symantec, among others, that work constantly against the threat of cyber crime, and provide customers with software that protects them. Arm yourself with the right anti-virus package, keep your operating system and your web browsers updated, and always browse the internet behind a firewall and your anti-virus switched on. Do not make online purchases from cyber cafes even if they're in secure locations, do not open email you don't trust, and do not engage in conversations online with strangers. Do not keep sensitive material on your computer without the right protection, and make sure to keep a record of your personal financial transactions. If you suspect any unusual activity, or something seems out of place, disconnect the internet at once, freeze the affected accounts and contact law enforcement immediately to stop further damage.

Misconceptions or scepticism about any sort of transactions across the internet considering all the illicit activity is understandable. However, many sites are also trustworthy and provide you with good service while making life easier for you due to easy access. But then protection is always necessary. The internet is a safe place to live in, as long as we're armed with the right equipment and know-how to avoid being a casualty. 



THE 12 TYPES OF CYBER CRIME

There are literally a dozen ways in which a cybercrime can be perpetrated, and you need to know what they are

In order to protect yourself you need to know about the different ways in which your computer can be compromised and your privacy infringed. In this section, we discuss a few common tools and techniques employed by the cyber criminals. This isn't an exhaustive list by any means, but will give you a comprehensive idea of the loopholes in networks and security systems, which can be exploited by attackers, and also their possible motives for doing so.

1. Hacking

In simple words, hacking is an act committed by an intruder by accessing your computer system without your permission. Hackers (the people doing the ‘hacking’) are basically computer programmers, who have an advanced understanding of computers and commonly misuse this knowledge for devious reasons. They’re usually technology buffs who have expert-level skills in one particular software program or language.

As for motives, there could be several, but the most common are pretty simple and can be explained by a human tendency such as greed, fame, power, etc. Some people do it purely to show-off their expertise – ranging from relatively harmless activities such as modifying software (and even hardware) to carry out tasks that are outside the creator’s intent, others just want to cause destruction.

Greed and sometimes voyeuristic tendencies may cause a hacker to break into systems to steal personal banking information, a corporation’s financial data, etc. They also try and modify systems so that they can execute tasks at their whims. Hackers displaying such destructive conduct are also called “Crackers” at times. They are also called “Black Hat” hackers.

On the other hand, there are those who develop an interest in computer hacking just out of intellectual curiosity. Some companies hire these computer enthusiasts to find flaws in their security systems and help fix them. Referred to as “White Hat” hackers, these guys are against the abuse of computer systems. They attempt to break into network systems purely to alert the owners of flaws. It’s not always altruistic, though, because many do this for fame as well, in order to land jobs with top companies, or just to be termed as security experts. “Grey Hat” is another term used to refer to hacking activities that are a cross between black and white hacking.

Some of the most famous computer geniuses were once hackers who went on to use their skills for constructive technological development. Dennis Ritchie and Ken Thompson, the creators of the UNIX operating system (Linux’s predecessor), were two of them. Shawn Fanning, the developer of Napster, Mark Zuckerberg of Facebook fame, and many more are also examples.

The first step towards preventing hackers from gaining access to your systems is to learn how hacking is done. Of course it is beyond the scope of this Fast Track to go into great details, but we will cover the various techniques used by hackers to get to you via the internet.

- a. **SQL Injections:** An SQL injection is a technique that allows hackers to play upon the security vulnerabilities of the software that runs a web site.

It can be used to attack any type of unprotected or improperly protected SQL database. This process involves entering portions of SQL code into a web form entry field – most commonly usernames and passwords – to give the hacker further access to the site backend, or to a particular user's account. When you enter logon information into sign-in fields, this information is typically converted to an SQL command. This command checks the data you've entered against the relevant table in the database. If your input data matches the data in the table, you're granted access, if not, you get the kind of error you would have seen when you put in a wrong password. An SQL injection is usually an additional command that when inserted into the web form, tries to change the content of the database to reflect a successful login. It can also be used to retrieve information such as credit card numbers or passwords from unprotected sites.

- b. **Theft of FTP Passwords:** This is another very common way to tamper with web sites. FTP password hacking takes advantage of the fact that many webmasters store their web site login information on their poorly protected PCs. The thief searches the victim's system for FTP login details, and then relays them to his own remote computer. He then logs into the web site via the remote computer and modifies the web pages as he or she pleases.
- c. **Cross-site scripting:** Also known as XSS (formerly CSS, but renamed due to confusion with cascading style sheets), is a very easy way of circumventing a security system. Cross-site scripting is a hard-to-find loophole in a web site, making it vulnerable to attack. In a typical XSS attack, the hacker infects a web page with a malicious client-side script or program. When you visit this web page, the script is automatically downloaded to your browser and executed. Typically, attackers inject HTML, JavaScript, VBScript, ActiveX or Flash into a vulnerable application to deceive you and gather confidential information.

If you want to protect your PC from malicious hackers, investing in a good firewall should be first and foremost. Hacking is done through a network, so it's very important to stay safe while using the internet. You'll read more about safety tips in the last chapter of this book.

2. Virus dissemination

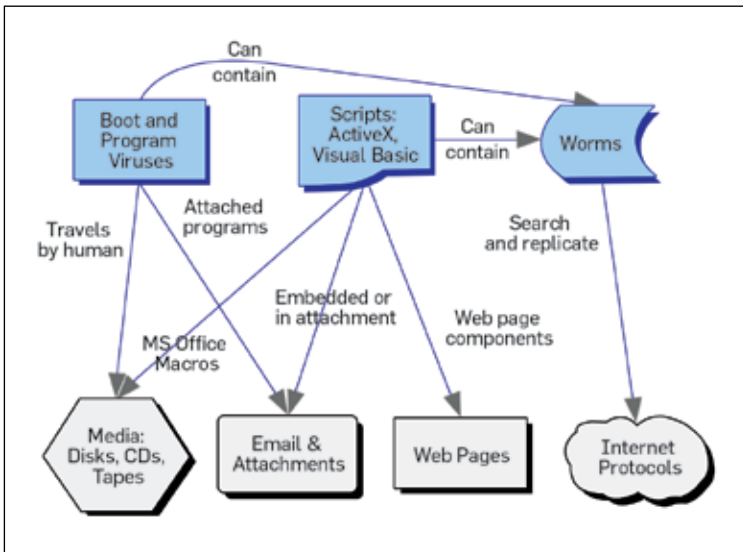
Viruses are computer programs that attach themselves to or infect a system or files, and have a tendency to circulate to other computers on a network.

They disrupt the computer operation and affect the data stored – either by modifying it or by deleting it altogether. “Worms” unlike viruses don’t need a host to cling on to. They merely replicate until they eat up all available memory in the system. The term “worm” is sometimes used to mean self-replicating “malware” (MALicious softWARE). These terms are often used interchangeably in the context of the hybrid viruses/worms that dominate the current virus scenario.

“Trojan horses” are different from viruses in their manner of propagation. They masquerade as a legitimate file, such as an email attachment from a supposed friend with a very believable name, and don’t disseminate themselves. The user can also unknowingly install a Trojan-infected program via drive-by downloads when visiting a web site, playing online games or using internet-driven applications. A Trojan horse can cause damage similar to other viruses, such as steal information or hamper/disrupt the functioning of computer systems.



Although mankind’s best invention, the net is still a minefield of threats



A simple diagram to show how malware can propagate

How does this happen? Well, the malicious code or virus is inserted into the chain of command so that when the infected program is run, the viral code is also executed (or in some cases, runs instead of the legitimate program). Viruses are usually seen as extraneous code attached to a host program, but this isn't always the case. Sometimes, the environment is manipulated so that calling a legitimate uninfected program calls the viral program. The viral program may also be executed before any other program is run. This can virtually infect every executable file on the computer, even though none of those files' code was actually tampered with. Viruses that follow this modus operandi include "cluster" or "FAT" (File Allocation Table) viruses, which redirect system pointers to infected files, associate viruses and viruses that modify the Windows Registry directory entries so that their own code is executed before any other legitimate program.

Computer viruses usually spread via removable media or the internet. A flash disk, CD-ROM, magnetic tape or other storage device that has been in an infected computer infects all future computers in which it's used. Your computer can also contract viruses from sinister email attachments, rogue web sites or infected software. And these disseminate to every other computer on your network.

All computer viruses cause direct or indirect economic damages. Based on this, there are two categories of viruses:

- 1) Those that only disseminate and don't cause intentional damage
- 2) Those which are programmed to cause damage.

However, even by disseminating, they take up plenty of memory space, and time and resources that are spent on the clean-up job. Direct economic damages are caused when viruses alter the information during digital transmission. Considerable expenses are incurred by individuals, firms and authorities for developing and implementing the anti-virus tools to protect computer systems.

3. Logic bombs

A logic bomb, also known as “slag code”, is a malicious piece of code which is intentionally inserted into software to execute a malicious task when triggered by a specific event. It's not a virus, although it usually behaves in a similar manner. It is stealthily inserted into the program where it lies dormant until specified conditions are met. Malicious software such as viruses and worms often contain logic bombs which are triggered at a specific payload or at a predefined time. The payload of a logic bomb is unknown to the user of the software, and the task that it executes unwanted. Program codes that are scheduled to execute at a particular time are known as “time-bombs”. For example, the infamous “Friday the 13th” virus which attacked the host systems only on specific dates; it “exploded” (duplicated itself) every Friday that happened to be the thirteenth of a month, thus causing system slowdowns.

Logic bombs are usually employed by disgruntled employees working in the IT sector. You may have heard of “disgruntled employee syndrome” wherein angry employees who've been fired use logic bombs to delete the databases of their employers, stultify the network for a while or even do insider trading. Triggers associated with the execution of logic bombs can be a specific date and time, a missing entry from a database or not putting in a command at the usual time, meaning the person doesn't work there anymore. Most logic bombs stay only in the network they were employed in. So in most cases, they're an insider job. This makes them easier to design and execute than a virus. It doesn't need to replicate; which is a more complex job. To keep your network protected from the logic bombs, you need constant monitoring of the data and efficient anti-virus software on each of the computers in the network.

There's another use for the type of action carried out in a logic bomb "explosion" – to make restricted software trials. The embedded piece of code destroys the software after a defined period of time or renders it unusable until the user pays for its further use. Although this piece of code uses the same technique as a logic bomb, it has a non-destructive, non-malicious and user-transparent use, and is not typically referred to as one.

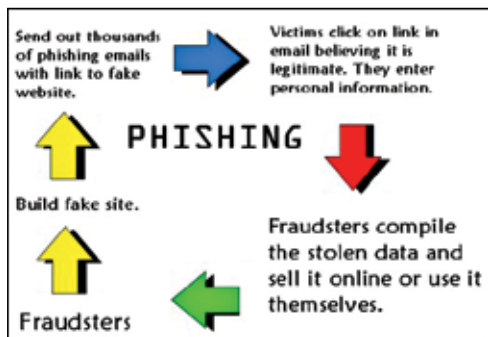
4. Denial-of-Service attack

A Denial-of-Service (DoS) attack is an explicit attempt by attackers to deny service to intended users of that service. It involves flooding a computer resource with more requests than it can handle consuming its available bandwidth which results in server overload. This causes the resource (e.g. a web server) to crash or slow down significantly so that no one can access it. Using this technique, the attacker can render a web site inoperable by sending massive amounts of traffic to the targeted site. A site may temporarily malfunction or crash completely, in any case resulting in inability of the system to communicate adequately. DoS attacks violate the acceptable use policies of virtually all internet service providers.

Another variation to a denial-of-service attack is known as a "Distributed Denial of Service" (DDoS) attack wherein a number of geographically widespread perpetrators flood the network traffic. Denial-of-Service attacks typically target high profile web site servers belonging to banks and credit card payment gateways. Web sites of companies such as Amazon, CNN, Yahoo, Twitter and eBay! are not spared either.

5. Phishing

This is a technique of extracting confidential information such as credit card numbers and username-password combos by masquerading as a legitimate enterprise. Phishing is typically carried out by email spoofing. You've probably



How phishing can net some really interesting catches

received email containing links to legitimate appearing websites. You probably found it suspicious and didn't click the link. Smart move. The malware would have installed itself on your computer and stolen private information. Cyber-criminals use social engineering to trick you into downloading malware off the internet or make you fill in your personal information under false pretenses.

A phishing scam in an email message can be evaded by keeping certain things in mind.

- ▶ Look for spelling mistakes in the text. Cyber-criminals are not known for their grammar and spelling.
- ▶ Hover your cursor over the hyperlinked URL but don't click. Check if the address matches with the one written in the message.
- ▶ Watch out for fake threats. Did you receive a message saying "Your email account will be closed if you don't reply to this email"? They might trick you by threatening that your security has been compromised.
- ▶ Attackers use the names and logos of well-known web sites to deceive you. The graphics and the web addresses used in the email are strikingly similar to the legitimate ones, but they lead you to phony sites.

Not all phishing is done via email or web sites. Vishing (voice phishing) involves calls to victims using fake identity fooling you into considering the call to be from a trusted organisation. They may claim to be from a bank asking you to dial a number (provided by VoIP service and owned by attacker) and enter your account details. Once you do that, your account security is compromised. Treat all unsolicited phone calls with skepticism and never provide any personal information. Many banks have issued preemptive warnings informing their users of phishing scams and the do's and don'ts regarding your account information. Those of you reading Digit for long enough will remember that we successfully phished hundreds of our readers by reporting a way to hack other people's gmail accounts by sending an email to a made up account with your own username and password... and we did that years ago in a story about , yes, you guessed it, phishing!

6. Email bombing and spamming

Email bombing is characterised by an abuser sending huge volumes of email to a target address resulting in victim's email account or mail servers crashing. The message is meaningless and excessively long in order to consume network resources. If multiple accounts of a mail server are targeted, it may have a denial-of-service impact.

Such mail arriving frequently in your inbox can be easily detected by spam filters. Email bombing is commonly carried out using botnets (private internet connected computers whose security has been compromised by malware and under the attacker's control) as a DDoS attack. This type of attack is more difficult to control due to multiple source addresses and the bots which are programmed to send different messages to defeat spam filters.

“Spamming” is a variant of email bombing. Here unsolicited bulk messages are sent to a large number of users, indiscriminately. Opening links given in spam mails may lead you to phishing web sites hosting malware. Spam mail may also have infected files as attachments. Email spamming worsens when the recipient replies to the email causing all the original addressees to receive the reply. Spammers collect email addresses from customer lists, newsgroups, chat-rooms, web sites and viruses which harvest users' address books, and sell them to other spammers as well. A large amount of spam is sent to invalid email addresses.



Email filters cleaning out spam mail

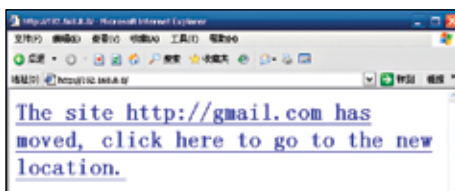
Sending spam violates the acceptable use policy (AUP) of almost all internet service providers. If your system suddenly becomes sluggish (email loads slowly or doesn't appear to be sent or received), the reason may be that your mailer is processing a large number of messages. Unfortunately, at this time, there's no way to completely prevent email bombing and spam mails as it's impossible to predict the origin of the next attack. However, what you can do is identify the source of the spam mails and have your router configured to block any incoming packets from that address.

7. Web jacking

Web jacking derives its name from “hijacking”. Here, the hacker takes control of a web site fraudulently. He may change the content of the original site or even redirect the user to another fake similar looking page controlled by him. The owner of the web site has no more control and the attacker may use the web site for his own selfish interests. Cases have been reported where the attacker has asked for ransom, and even posted obscene material on the site.

The web jacking method attack may be used to create a clone of the web site, and present the victim with the new link saying that the site has moved.

Unlike usual phishing methods, when you hover your cursor over the link provided, the URL presented will be the original one, and not the attacker's site. But when you click on the new link, it opens



Obviously not gmail.com, but still enough people click

and is quickly replaced with the malicious web server. The name on the address bar will be slightly different from the original web site that can trick the user into thinking it's a legitimate site. For example, "gmail" may direct you to "gmail". Notice the one in place of 'L'. It can be easily overlooked.

Web jacking can also be done by sending a counterfeit message to the registrar controlling the domain name registration, under a false identity asking him to connect a domain name to the webjacker's IP address, thus sending unsuspecting consumers who enter that particular domain name to a web site controlled by the webjacker. The purpose of this attack is to try to harvest the credentials, usernames, passwords and account numbers of users by using a fake web page with a valid link which opens when the user is redirected to it after opening the legitimate site.

8. Cyber stalking

Cyber stalking is a new form of internet crime in our society when a person is pursued or followed online. A cyber stalker doesn't physically follow his victim; he does it virtually by following his online activity to harvest information about the stalkee and harass him or her and make threats using verbal intimidation. It's an invasion of one's online privacy. Cyber stalking uses the internet or any other electronic means and is different from offline stalking, but is usually accompanied by it. Most victims of this crime are women who are stalked by men and children who are stalked by adult predators and pedophiles. Cyber stalkers thrive on inexperienced web users who are not well aware of netiquette and the rules of internet safety. A cyber stalker may be a stranger, but could just as easily be someone you know.

Cyber stalkers harass their victims via email, chat rooms, web sites, discussion forums and open publishing web sites (e.g. blogs). The availability of free email / web site space and the anonymity provided by chat rooms and forums has contributed to the increase of cyber stalking incidents. Everyone has an

online presence nowadays, and it's really easy to do a Google search and get one's name, alias, contact number and address, contributing to the menace that is cyber stalking. As the internet is increasingly becoming an integral part of our personal and professional lives, stalkers can take advantage of the ease of communications and the availability of personal information only a few mouse clicks away. In addition, the anonymous and non-confrontational nature of internet communications further tosses away any disincentives in the way of cyber stalking.

Cyber stalking is done in two primary ways:

- ▶ **Internet Stalking:** Here the stalker harasses the victim via the internet. Unsolicited email is the most common way of threatening someone, and the stalker may even send obscene content and viruses by email. However, viruses and unsolicited telemarketing email alone do not constitute cyber stalking. But if email is sent repeatedly in an attempt to intimidate the recipient, they may be considered as stalking. Internet stalking is not limited to email; stalkers can more comprehensively use the internet to harass the victims. Any other cyber-crime that we've already read about, if done with an intention to threaten, harass, or slander the victim may amount to cyber stalking.
- ▶ **Computer Stalking:** The more technologically advanced stalkers apply their computer skills to assist them with the crime. They gain unauthorised control of the victim's computer by exploiting the working of the internet and the Windows operating system. Though this is usually done by proficient and computer savvy stalkers, instructions on how to accomplish this are easily available on the internet.

Cyber stalking has now spread its wings to social networking. With the increased use of social media such as Facebook, Twitter, Flickr and YouTube, your profile, photos, and status updates are up for the world to see. Your online presence provides enough information for you to become a potential victim of stalking without even being aware of the risk. With the "check-ins", the "life-events", apps which access your personal information and the need to put up just about everything that you're doing and where you're doing it, one doesn't really leave anything for the stalkers to figure out for themselves. Social networking technology provides a social and collaborative platform for internet users to interact, express their thoughts and share almost everything about their lives. Though it promotes socialisation amongst people, along the way it contributes to the rise of internet violations.

9. Data diddling

Data Diddling is unauthorised altering of data before or during entry into a computer system, and then changing it back after processing is done. Using this technique, the attacker may modify the expected output and is difficult to track. In other words, the original information to be entered is changed, either by a person typing in the data, a virus that's programmed to change the data, the programmer of the database or application, or anyone else involved in the process of creating, recording, encoding, examining, checking, converting or transmitting data.

This is one of the simplest methods of committing a computer-related crime, because even a computer amateur can do it. Despite this being an effortless task, it can have detrimental effects. For example, a person responsible for accounting may change data about themselves or a friend or relative showing that they're paid in full. By altering or failing to enter the information, they're able to steal from the enterprise. Other examples include forging or counterfeiting documents and exchanging valid computer tapes or cards with prepared replacements. Electricity boards in India have been victims of data diddling by computer criminals when private parties were computerizing their systems.

10. Identity Theft and Credit Card Fraud

Identity theft occurs when someone steals your identity and pretends to be you to access resources such as credit cards, bank accounts and other benefits in your name. The imposter may also use your identity to commit other crimes.



Credit card fraud is the most common way for hackers to steal your money

“Credit card fraud” is a wide ranging term for crimes involving identity theft where the criminal uses your credit card to fund his transactions. Credit card fraud is identity theft in its simplest form. The most common case of credit card fraud is your pre-approved card falling into someone else's hands. He can use it to buy anything until you report to the authorities and get your card blocked. The only security measure on credit card purchases is the signature on the receipt but that can very easily be forged. However, in some countries the

merchant may even ask you for an ID or a PIN. Some credit card companies have software to estimate the probability of fraud. If an unusually large transaction is made, the issuer may even call you to verify.

Often people forget to collect their copy of the credit card receipt after eating at restaurants or elsewhere when they pay by credit card. These receipts have your credit card number and your signature for anyone to see and use. With only this information, someone can make purchases online or by phone. You won't notice it until you get your monthly statement, which is why you should carefully study your statements. Make sure the website is trustworthy and secure when shopping online. Some hackers may get a hold of your credit card number by employing phishing techniques.

Sometimes a tiny padlock icon appears on the left screen corner of the address bar on your browser which provides a higher level of security for data transmission. If you click on it, it will also tell you the encryption software it uses.

A more serious concern is the use of your personal information with the help of stolen or fake documents to open accounts (or even worse, using your existing account) to take a loan in your name. These unscrupulous people can collect your personal details from your mailbox or trash can (remember to shred all sensitive documents). Think of all the important details printed on those receipts, pay stubs and other documents. You won't know a thing until the credit card people track you down and tail you until you clear all your dues. Then for months and months you'll be fighting to get your credit restored and your name cleared.

With rising cases of credit card fraud, many financial institutions have stepped in with software solutions to monitor your credit and guard your identity. ID theft insurance can be taken to recover lost wages and restore your credit. But before you spend a fortune on these services, apply the no-cost, common sense measures to avert such a crime.

11. Salami slicing attack

A "salami slicing attack" or "salami fraud" is a technique by which cyber-criminals steal money or resources a bit at a time so that there's no noticeable difference in overall size. The perpetrator gets away with these little pieces from a large number of resources and thus accumulates a considerable amount over a period of time. The essence of this method is the failure to detect the misappropriation.

The most classic approach is "collect-the-roundoff" technique. Most calculations are carried out in a particular currency are rounded off *up* to

the nearest number about half the time and *down* the rest of the time. If a programmer decides to collect these excess fractions of rupees to a separate account, no net loss to the system seems apparent. This is done by carefully transferring the funds into the perpetrator's account.

Attackers insert a program into the system to automatically carry out the task. Logic bombs may also be employed by unsatisfied greedy employees who exploit their know-how of the network and/or privileged access to the system. In this technique, the criminal programs the arithmetic calculators to automatically modify data, such as in interest calculations.

Stealing money electronically is the most common use of the salami slicing technique, but it's not restricted to money laundering. The salami technique can also be applied to gather little bits of information over a period of time to deduce an overall picture of an organisation. This act of distributed information gathering may be against an individual or an organisation. Data can be collected from web sites, advertisements, documents collected from trash cans, and the like, gradually building up a whole database of factual intelligence about the target.

Since the amount of misappropriation is just below the threshold of perception, we need to be more vigilant. Careful examination of our assets, transactions and every other dealing including sharing of confidential information with others might help reduce the chances of an attack by this method.

12. Software Piracy

Thanks to the internet and torrents, you can find almost any movie, software or song from any origin for free. Internet piracy is an integral part of our lives which knowingly or unknowingly we all contribute to. This way, the profits of the resource developers are being cut down. It's not just about using someone else's intellectual property illegally but also passing it on to your friends further reducing the revenue they deserve.



Piracy is rampant in India, but you knew that

Software piracy is the unauthorised use and distribution of computer software. Software developers work hard to develop these programs, and piracy curbs their ability to generate enough

revenue to sustain application development. This affects the whole global economy as funds are relayed from other sectors which results in less investment in marketing and research.

The following constitute software piracy:

- ▶ Loading unlicensed software on your PC
- ▶ Using single-licensed software on multiple computers
- ▶ Using a key generator to circumvent copy protection
- ▶ Distributing a licensed or unlicensed (“cracked”) version of software over the internet and offline

“Cloning” is another threat. It happens when someone copies the idea behind your software and writes his own code. Since ideas are not copy protected across borders all the time, this isn’t strictly illegal.

A software “crack” is an illegally obtained version of the software which works its way around the encoded copy prevention. Users of pirated software may use a key generator to generate a “serial” number which unlocks an evaluation version of the software, thus defeating the copy protection. Software cracking and using unauthorised keys are illegal acts of copyright infringement.


Using pirated material comes with its own risks. The pirated software may contain Trojans, viruses, worms and other malware, since pirates will often infect software with malicious code. Users of pirated software may be punished by the law for illegal use of copyrighted material. Plus you won’t get the software support that is provided by the developers.

To protect your software from piracy if you’re a developer, you should apply strong safeguards. Some web sites sell software with a “digital fingerprint” that helps in tracing back the pirated copies to the source. Another common method is hardware locking. Using this, the software license is locked to a specific computer hardware, such that it runs only on that computer. Unfortunately, hackers continue to find their way around these measures.

13. Others

So far we’ve discussed the dedicated methods of committing cyber crimes. In a nutshell, any offence committed using electronic means such as net extortion, cyber bullying, child pornography and internet fraud is termed as cyber crime.

The internet is a huge breeding ground for pornography, which has often been subject to censorship on grounds of obscenity. But what may be considered obscene in India, might not be considered so in other countries.

Since every country has a different legal stand on this subject matter, pornography is rampant online. However, according to the Indian Constitution, largely, pornography falls under the category of obscenity and is punishable by law. Child pornography is a serious offence, and can attract the harshest punishments provided for by law. Pedophiles lurk in chat rooms to lure children. The internet allows long-term victimisation of such children, because the pictures once put up, spread like wild-fire, and may never get taken down completely. Internet crimes against children are a matter of grave concern, and are being addressed by the authorities, but this problem has no easy solution. 



HOW TO TELL IF YOU'RE A VICTIM OF CYBER CRIME

Without you knowing it, you may be a victim of cybercrime. Here are simple things you can do to find out if you've been compromised

In the previous chapter, you were introduced to some of the most important weapons used by cybercriminals to bring their imaginations to reality. Now, you'll learn how to detect whether you're a victim of (or on the verge of being a victim of) cyber crime by

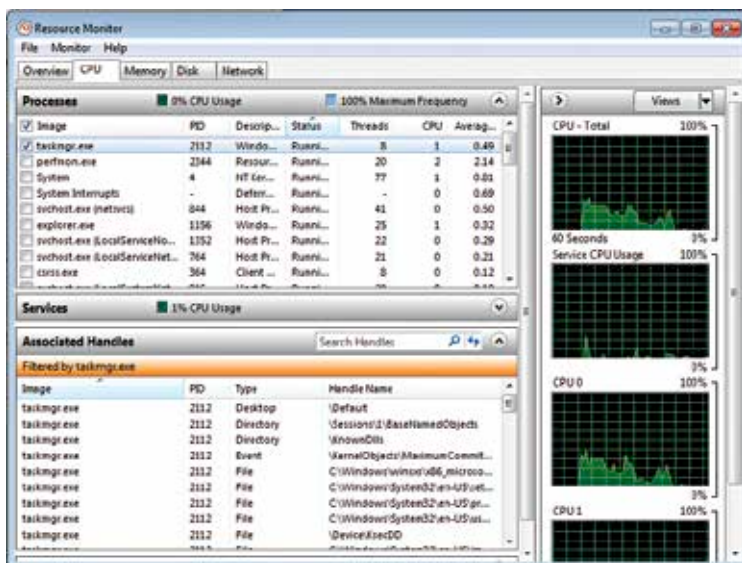
watching out for suspicious activity. Let's look at the most common types of cyber crime attacks.

Viruses (and other malware)

Viruses are software too, however they're malicious. A virus would always need to run to make an impact. Unless a virus is executed, the file itself remains completely harmless. Then again it isn't possible to keep checking all the processes running on your system. What you can do is detect the symptoms of viral activities.

Looking beyond the facade

Viruses create problems by overutilizing resources. The four primary resources in a computer system are CPU, disk (hard disk) and RAM. Many viruses slow down the computer by either putting the CPU at full use or consuming too much RAM even when the computer is idle. Both these cases can be detected using Windows Task Manager and you can kill any process that looks suspicious. However virus creators have learnt a workaround to this: At times, they name the virus' executable file to make it look like one of the important executable files in Windows. The most common name used is



Resource Monitor is a great tool to keep a tab on what's going on in your system

“svchost.exe” which usually runs in multiple instances and together hosts many services running on the system. Do note that the paths of viruses will differ from those of the original files.

Besides file name, also look at the file size and network bandwidth in Task Manager. If there's a virus which creates a swarm of files in hidden system directories (such as in 'System Volume Information' folder on each partition/volume) then it would be utilizing plenty of disk space. Or if it comes with a malware which transfers your personal files from your documents library to a remote server then it would be utilizing network bandwidth.

Windows Vista and all higher versions of Windows come equipped with a very capable software named “Resource Monitor”. Launch it and you'll find yet another way to keep an eye on the processes in your system.

Auto-vigilance with anti-virus

Though these are some basic countermeasures, they won't work for some viruses e.g. those which are not meant to slow down PCs but to destroy data. We recommend you get an anti-virus and keep it updated; an internet connection is necessary for updation purpose. Avast anti-virus is effective and is legally free for home use; it provides a lot of flexibility and control. If you have money to spend to ensure security for any sensitive files on your computers, we'd say get yourself a protection suite for they come with more than just anti-virus software. Yet another defense is not running the computer as an administrator. Though UAC on Windows Vista and above provide a good level of security, an accidental click on a 'yes' in a random pop-up might allow a malicious code to execute. If you're vigilant enough, you should be fine because a virus can't cause much havoc on your computer unless it gains administrative rights. If you don't have an updated anti-virus, a virus without administrative privileges still leaves a window of escape for you – you can create a new account on the computer, transfer your documents to it and use that account instead!

Viruses enter via either removable media or the internet. Remain vigilant enough and do not install just about any software because, say, it promises you a larger set of smilies in Google Talk. Most (if not all) such software come bundled with viruses. Stay away from cracked software; always download patches and updates from the official vendors. A good browser which offers more security is better. We recommend Google Chrome, Mozilla Firefox and Opera compared to Internet Explorer for two reasons: i) Chrome and Firefox are more updated to the new HTML5 standards and ii) they're not deeply

embedded into Windows thus making sure that a vulnerability doesn't go too deep. Remember one fact: monitoring viral activities manually is always a lot tougher than updating your anti-virus regularly. One should always be ready to counter an infection manually but having an anti-virus protects you most of the time.

Denial of Service attacks

Denial of Service (or DoS) attacks happen via the internet. They're carried out by opening many connections to your computer and leaving them open; this consumes plenty of resources on your computer and can crash it. Though your internet connection will go bonkers before a crash, it's difficult to detect DoS because its strength lies in bombarding the computer with connection requests at a very high speed. So before you can discover what went wrong, the system would have already gotten too slow to start monitoring it.

Knowing when you've been, well, denied service

You can either get yourself a firewall package or use Windows Firewall which can normally prevent such scenarios.

We won't explain how to use them in detail since they're beyond the scope of this book and require a sound explanation of how the TCP protocol works. No need to sweat though; not only will Windows Firewall be able to defend you well, chances are high that you'll never face a DoS attack in the first place for two reasons: most ISPs use dynamic IP addresses (every time you connect, your public IP address changes) and most ISPs put you behind a NAT (Network Address Translation). Though they do it to save IP address consumption, it ends up protecting you as your public IP address maps to many people at the same time. If you're still afraid, get yourself a firewall package and relax.

Hacking

Just as in case of DoS, it's very difficult to discover signs of hacking once it's done since a

NOTE

In Windows Firewall with Advanced Security, you can create a rule which blocks all incoming connections on all TCP ports and keep the rule deactivated. If you detect a DoS, activate the rule to enable protection. Remember that enabling such a rule can disturb operations of a lot of software as well as web pages though it should not completely make your net connection useless.

clever hacker won't leave traces and cause for suspicion. Everything he does is done behind the scenes, and there's no simple way to know if you've been a target. Prevention is the cure again. Though malicious hacking is usually called cracking, crackers prefer the term hackers. Coming to what matters, hacking can be done in two ways:

- 1 **Locally:** using the same computer which needs to be compromised.
- 2 **Remotely:** hacking the computer over a network.

FTP server software vulnerabilities

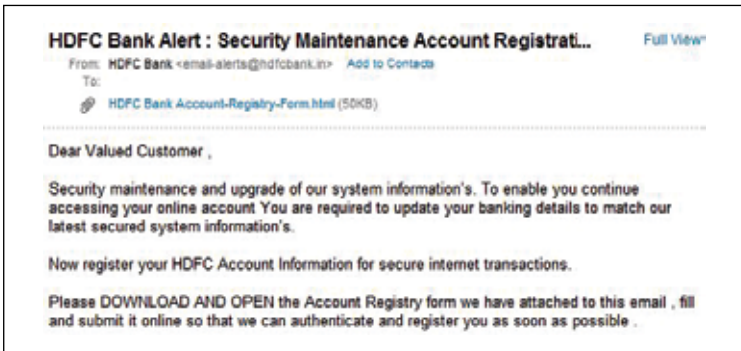
Once your computer is in the wrong hands, well the game is already over. Not so easily though. To hack over a network, the hacker needs to know your IP address. Since most ISPs implement NAT, a basic level of protection is already there. But that's not enough. Hacking over a network requires an exploitable service to be running on your system. For example, if you have FTP server software running on your system and there are known weaknesses in the software, then you're vulnerable to attack. Once again, intelligent rules on your firewall can help with this. In most cases, Windows Firewall has rules potent enough to guard you against intruders. However, it's recommended that you open each service for only those IP ranges from which you expect a connection. For example, if the FTP service is meant for being used only on the home network then you can specify the IP address range in Windows Firewall for which the FTP service should be available.

Keep your friends close, but your enemies closer

Though chances that you would be selected randomly by a malicious hacker are very low (directly proportional to your enemy count), extra precautions never hurt. Some servers such as database servers and web servers can be configured to work only on certain interfaces (e.g. you can disable them for wireless networks). But this solution works in rare cases. On most instance, a more well known program is targeted; for example a vulnerability in day-to-day software such as Firefox, Internet Explorer, Google Talk etc. can allow hackers to take control of your computer. So keep updating them and your OS regularly to have the latest improvements and security.

Phishing

How do you find out if you're being phished? Well, the answer is: keep your eyes open. Phishing tricks you into opening a malicious site designed to



Sample phishing email

look (and at times behave) similar to original site. Often it's done via URLs which look very similar to the original site. e.g. if you're a customer of HDFC Bank you may receive an email asking you to change your password with a link that takes you to netbanking.hdfc-bank.com.

If you were sharp enough you probably noticed two things just now:

1. The website for HDFC Bank is not hdfc-bank.com but hdfcbank.com
2. Banks rarely email their customers asking them to log in to their online accounts.

Time to change your password?

Remember that most organizations dealing with money (banks, payment gateways, payment services such as Paypal etc.) never ask you to change your password or verify your account/credit card/debit card via a call or email. So don't fall for these tricks. Most phishing email contain non-professional and incorrect English. That should be your first cue, but there's more.

Make your (book)mark

The main defense against phishing is your gut instinct. Also, never type addresses into the URL bar manually. Use the bookmarks feature of browsers to save addresses and use them – this prevents a spelling mistake from developing into a financial injury. Memorize your bank's web address well and crosscheck the URL before entering any credentials. Again, banking websites (and others dealing with money) use [HTTPS](https://) (secure [HTTP](https://)). So do check for that when browsing. You may want to have a look at the certificate

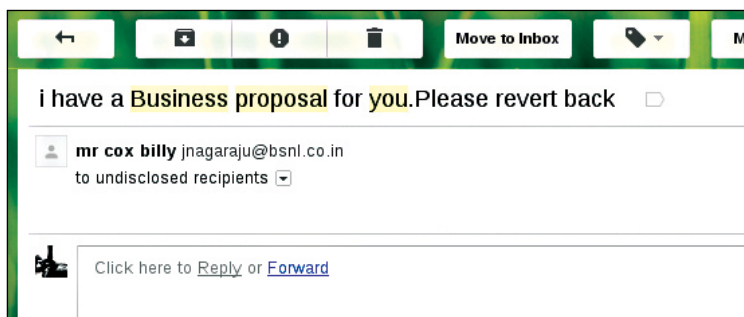
as well. Googling the site name and then opening the site via a result is also a good way to avoid phishing traps but the final defense lies in observing the correct address. Better safe than sorry.

Pharming

Pharming is an attack intended to redirect your website traffic to another, probably bogus website. Sad news: pharming is not easily detectable on your computer. Pharming is usually done by infecting DNS servers which is beyond control and remains undetectable for a large part. The only way pharming could have been done on your computer is by modifying the hosts file. If that file contains bogus entries then some program has tried to perform pharming on your computer. Some site blocking software use the hosts file to map addresses to localhost. Hence, if a web address is being mapped to anything other than 127.0.0.1 (IPv4 loopback address) or ::1 (IPv6 loopback address) in the hosts file, it's indicative of pharming (unless of course, you added an entry in the file).

Spam

Computers have become more intelligent, as have spammers. While in the past, you encountered spam in the form of long email from anonymous people claiming to be heirs of large empires, the trick is now more simple. Spammers now send a very concise email saying "I have a business proposal for you" asking you to revert. Such email is usually sent from unknown email addresses and strange names. Don't get too inquisitive and reply back. It might just lead into a similar situation which would be caused by replying to anonymous heirs of unknown empires.



Make a note of name, email address and content before you reply

Threats against your online presence

If you're sure that you didn't change your password or make a typing mistake and yet Gmail says that your password was recently changed, your account is no longer yours. This, however, is not the only way by which you could lose control of your online presence.

Facebook is not all rainbows and butterflies

If an unknown app for your computer can be a virus, a Facebook app can also be one. In this case, it won't disturb your computer but your online presence. These apps can be built by anyone and be hosted anywhere. Though they're part of Facebook's ecosystem, the social network doesn't take any responsibility for their activities. You do! Depending on what permissions you have given to a Facebook app, it can read your posts, post on your friends' walls on your behalf, read your profile information, your friends' profile information and store it on a different server. That can be a serious threat to you as well as your online friends. Before giving permissions to any app, ask yourself two questions:

1. Do I need this app?
2. Do I trust the creator of this app?

If you say no to either one, do not authorize an app. Even if you have to, carefully read what permissions you're granting the app. Similar rules apply for third-party Twitter apps.

Passwords – change them regularly for Lee's sake

Ever since Tim Berners Lee invented the web, email and then webmail has been one of the biggest revolutions in business and communication. If anyone were to gain access to your email account and send out unwanted emails, you would have to take the heat. You wouldn't even have evidence of the sent mail in your outbox and your relationships might sour before you know it.

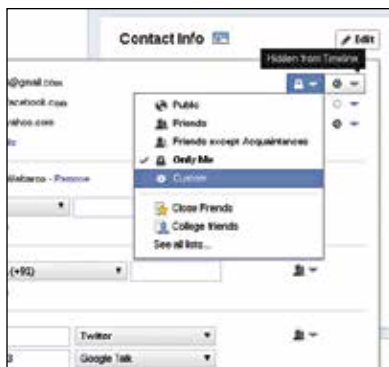
Gmail allows you to see your other “active sessions” with locations from where the account was accessed. If you see any suspicious activity, log out of all other sessions and change your password immediately. One of the changes that an unauthorized accessor of your account would do is change the answer to your security question. It's a wise idea to check if the ‘forgot password’ feature works.

Your personal data is worth money

We're sure many geeks would have had this question asked of them: “Could

you hack a Facebook account if I asked you to?" There are people who want to know what you're doing and where you're doing it. They want to know your email address to sell it to companies who want to advertise their services to you at no cost. They want to know your mobile number to send you marketing messages. Remember not to disclose such information in public. Make sure your Facebook, Twitter and Google+ privacy settings are tight. If they're not, stop reading this and fix it right away. Remember that public personal data can be misused to impersonate you. Let's look at a hypothetical scenario.

All your personal information is set to 'public' on Facebook. An impersonator copies all that data (well, except the email address) and creates a duplicate profile. He then tells all your friends that your original account was hacked and you had to create a new account. Whom should your friends trust? Though some might want




Keep Facebook privacy settings tight

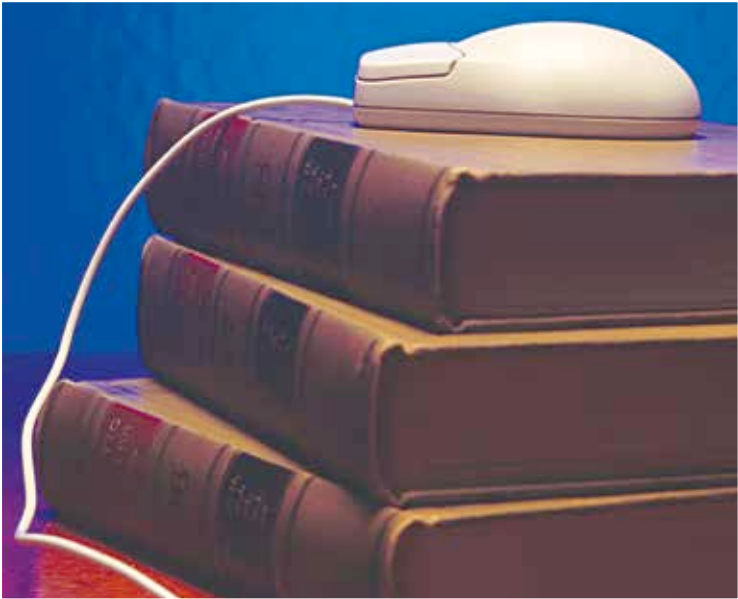
to have a second look at your email address, many would accept a friend request being sent by the fake account. This is why being reserved about sharing all your information protects not only you but also your friends. We recommend you organize your friends in groups (or circles) and allow only certain groups to view certain type of information about yourself.

Facebook was meant for friends, not stalkers

Friendship is the core around which Facebook was built but some users in a bid to increase the number of their 'friends' or to expand their friends circle accept friend invitations from even complete strangers. Facebook is a service which tries to bring the day-to-day social experience online. Accepting just about anyone's friend request is not the way to go about it. Doing this only makes your profile and data visible to a lot of unwanted users. It makes you an easy target for cyberstalkers.

Let's say you accepted a friend request from an account unknown to you. This might encourage the person to create yet another account and start talking to you online via multiple accounts which might end up in

you giving random details of your life to unknown people. This, in turn can be used to harass or blackmail you – or in short, for cyberstalking. If you were dumb enough to make personal information accessible to the unknown account, a clever social engineering attempt would be made on claims to your entire identity. So please beware. 



INDIAN CYBERCRIME LAWS

How is cybercrime policed in the
Indian context and what laws govern
Indian cyberspace

A real-world scenario

If your mixer-grinder refused to start one day despite your best efforts, and knowing that you haven't fiddled around with any critical piece of the machinery, would you keep trying to start it, or approach an electrician? What would you do when he tells you that you've been sold a defective piece?

Wouldn't your first thought be to take the device back to the outlet where you bought it from, and demand a replacement or a refund?

But when your spreadsheet software (which you have purchased legally) continues to crash throughout the day, regardless of the file you open, the setting you tweaked, or the programs you closed to free up memory, do you ever think about asking the software company for a refund? What causes this distinction between our experiences with offline and online products and services?

You would have noticed, as you try to install any software, that it asks you to read its "Terms and Conditions" (T&C), and indicate that you accept them by clicking on check box. You simply cannot install the software without accepting the T&C. But how many of us even view the T&C, leave alone actually reading the 1000 word manuscripts?

One prime difference lies in the fact that we have seen stuff like home appliances and electronic goods for the past five decades, while the computer and internet have been with us only since the last twenty years, cyber laws are an even newer kid on the block.

The Internet: Its everywhere...

The fact that the internet pervades most aspects of our lives today, means that an increasing number of people have a parallel electronic existence. With millions of individuals interacting with each other, consuming online ser-



vices, performing monetary transactions, and building viewpoints through cyberspace, monitoring, controlling, and policing the internet has become one of the prime concerns of almost all gov-

ernments worldwide. The anonymous, decentralized and instantly "live" nature of the internet makes it that much tougher to assign responsibility, draw up jurisdictions, and effectively resolve genuine grievances.

Increasing cases of criminal activities being conducted through this medium have been a growing concern and need to be tackled efficiently if we are ever to harness the true potential of the internet and convince even the most reluctant individuals in being connected to it.

A law behind every move you make

Every activity in the real world (e.g., buying a ticket, paying for groceries, signing an employment contract, etc.) has a legal underpinning. We rarely, if ever, consider the legal ramifications of our offline activities, because we are seldom the victims of a crime of fraud and resort to using the legal infrastructure (police, lawyers, courts) to resolve our grievances. The same applies to any online activity. The underlying thought behind every email we reply to, every twitter post we re-tweet, every net-banking transaction we perform, or every news article we read is that it is “legal” to do so. So what happens when someone does something illegal online. But even prior to that, how do we know whether something is really illegal.



What are cyberlaws?

“Cyberlaw or Internet law is a term that encapsulates the legal issues related to use of the Internet. It is less a distinct field of law than intellectual property or contract law, as it is a domain covering many areas of law and regulation.” (source: Wikipedia)

Cyberlaws, same as any other branch of law, help define what is legal and illegal, and stipulate mechanisms to detect, convict and punish offenders, and protect electronic property and its rightful use.

Cyberlaws pertain to diverse aspects of the electronic world such as:

- ▶ software licences, copyright and fair use
- ▶ unauthorized access, data privacy and spamming
- ▶ export of hardware and software
- ▶ censorship
- ▶ computerized voting

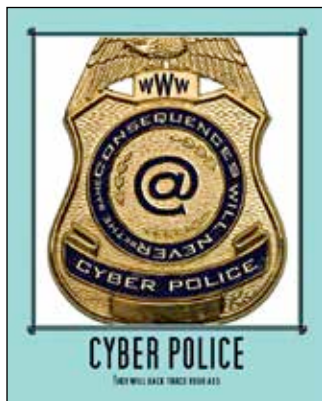
IT Act, 2000 and IT (Amendment) Act, 2008

These two pieces of legislation form the bedrock of cyberlaw infrastructure in India.

The Information Technology (IT) Act, 2000 was passed by the Indian Parliament in May 2000 and came into force in October of the same year.

Its prime purpose is to provide the legal infrastructure for e-commerce in India. It was the first legal instrument to provide legal sanctity to electronic records and contracts expressed through electronic means of communication. The act was later amended in December 2008 through the IT (Amendment) Act, 2008. Some of their salient points are:

- ▶ **Digital Signatures:** Electronic records may be authenticated by a subscriber by affixing digital signatures; further, the signature may be verified using the public key provided by the subscriber
- ▶ **Certifying Authorities:** domestic and foreign certifying authorities (which provide digital signature certificates) are recognized by the law; a “Controller of Certifying Authorities” shall supervise them
- ▶ **Electronic governance:** Documents required as per law by any arm of the government may be supplied in electronic form, and such documents are to be treated the same as handwritten, typewritten or printed documents
- ▶ **Offences and Penalties:** An Adjudicating Officer shall judge whether a person has committed an offence in contravention of any provision of the IT Act, 2000; the maximum penalty for any damage to computers or computer systems is a fine up to ₹1 crore
- ▶ **Appellate Tribunals:** A Cyber Regulations Appellate Tribunal shall be formed which shall hear appeals against orders passed by the Adjudicating Officers
- ▶ **Investigation:** Offences shall only be investigated by a police officer of the rank of the Deputy Superintendent of Police or above (amended to the rank “Inspector” or above by the IT (Amendment) Act, 2008)
- ▶ **Amendments to other laws:** Other acts such as the Indian Penal Code, 1860, the Indian Evidence Act, 1872, the Bankers’ Books Evidence Act, 1891, the Reserve Bank of India Act, 1934 were to be amended to align them with the IT Act
- ▶ **Network Service Providers:** Intermediaries in the data transmission process, such as Internet Service Providers, are not liable in certain cases, so long as the intermediary expeditiously acts to prevent the cybercrime on getting such instruction from the Government or its agency.



Why were these laws enacted?

As a result of the technological advancements in the IT industry, computers and internet became accessible to the common man in our country quite rapidly. Like any technology, IT too met with two kinds of people -- the users and the abusers. While cases of hacking came to light and identity, privacy and information security was found to be increasingly compromised by the new IT revolution, the need was felt for law and order mechanism in the electronic world too.



What offences are covered under these laws?

One viewpoint considered when drafting the IT Amendment Act, 2008, was that it should be a comprehensive piece of legislation with minimal dependence on other penal laws. Although this recommendation seems to have been overlooked, several new offences have been defined in the 2008 version. The two IT Acts together define the below offences and also recommend punishments for each of them:

1. Hacking

It is not defined in either of the IT Acts, which in itself may have considerably weakened the cybercrime legislation in India.

2. Data theft

This offence is defined as copying or extracting information from a computer system without the owners, including computer theft and theft of digital signals during transmission.

3. Identity theft (including Password Theft)

As per the IT (Amendment) Act 2008, this offence is defined as fraudulently

or dishonestly making use of the electronic signature, password, or any other unique identification feature of a person.

4. Email spoofing

This is commonly used by hackers to hide the actual email address from which phishing and spam message are sent. It may also be used in conjunction with other fraudulent methods to trick users into providing personal/confidential information.

5. Sending offensive messages

The IT Act defines this offense as sending offensive or false information for the purpose of causing hatred, ill will, etc.

6. Voyeurism

This is defined as publishing/transmitting of “compromising” images/videos of a person without his/her consent.

7. Child pornography

This covers offences against all individuals who have not completed 18 years of age. Despite being one of the most serious offences, it does not attract any severe punishment

8. Cyber terrorism

The addition of this offence was a major difference between the two IT Acts. Cyber terrorism is described in fair detail as denying access to a computer, attempting to access a computer resource without authorization, or contaminating a computer system.



Punishment

While all other offences are punishable by imprisonment up to 3-5 years and/or a fine of up to ₹3-5 Lakh, an individual convicted of cyberterrorism is punishable by imprisonment for life.

Who enforces the law? Where do I file a complaint?

What should you do if the password to your email account is stolen? Or if everyone on your Facebook friends list are receiving spam messages from your account? You may start by filing a complaint with the local police station.

A major positive of the IT (Amendment) Act, 2008 over the original IT Act, 2000 was that police officers of the rank of “Inspector” or above were empowered to investigate cyber crimes, as against the rank of “Deputy Superintendent of Police” or above required by the original Act. This would have, at least theoretically, considerably increased the bandwidth of enforcement agencies in handling cybercrimes. However, try not to cross any fingers or toes hoping that you’d get your email account back, as you shall see in the next section.

Here are some examples of cybercrime-fighting infrastructure set up in different parts of India:

1. India’s first exclusive cybercrime enforcement setup was the Cyber Crime Police Station set up in Bangalore
2. This was followed up by a similar police station in Andhra Pradesh, which functions from Hyderabad city and has statewide jurisdiction

Image Courtesy: The Hindu



Police officers attending an orientation programme on cyber laws

3. Cyber Crime Investigations Cells have also been set up by police departments of Mumbai, Kolkata and Tamil Nadu

Have these laws really helped us?

The conviction rate for cybercrimes in India has been less than 10 convictions in the last 12 years since the IT Act came into force (<http://dgit.in/UVeIT8>). Further, there have been zero convictions after IT (Amendment) Act, 2008 was implemented.

A serious drawback of current cybercrime legislation is that all offences, except cyber terrorism, are bailable. This allows ample leeway for guilty individuals to destroy all electronic evidence of their crimes as soon as they have attained bail. This “non-serious” approach to cyber crime has led to most people as well as enforcement agencies losing faith in the legislation itself, and contributed to the extremely low conviction rate. One cannot really blame the inspector at your neighbourhood for not being too keen on registering a cyber crime case, now can we?

Prominent cybercrime cases:

1. First conviction for a cybercrime in India

A call center employee at Noida had gained access to to an American citizen's credit card information and used the same to purchase a color television and a cordless phone through a Sony Entertainment website catering to NRIs. A month after the items were delivered to the individual, Sony Entertainment was informed by the credit card agency that the card owner had denied making the purchase. Luckily, digital photographs taken at the time of delivery were evidence enough for the CBI to convict the individual under several sections of the Indian Penal Code.

2. First conviction under the IT Act, 2000

Obscene and defamatory messages regarding a divorced woman were posted on a Yahoo message group, which resulted in phone calls to the woman in the belief that she was soliciting. Investigating based on a complaint made by the victim in February 2004, the police traced the source of the message to a Mumbai resident who was a family friend of the victim. He had resorted to harassing the victim as she had rejected his marriage offer. The accused's lawyers argued that the offending messages might have been sent by either the victim's ex-husband or by the victim herself in order to implicate the accused, and that the documentary evidence was not sustainable under the

Indian Evidence Act. However, the court found the accused guilty based on the statements by the Cyber Cafe owner where the messages originated as well as expert witness provided by Naavi. The accused was sentenced to rigorous imprisonment for 2 years and fine ₹5000.

3. Hackers deface the official website of the Maharashtra Government

The website <http://www.maharashtragovernment.in>, which contains details about government departments, circulars, reports, and several other topics, was hacked on 20 September 2007. Sources believed the hackers to be from Washington, USA, although, the hackers identified themselves as “Hackers Cool Al-Jazeera” and claimed they were based in Saudi Arabia, which authorities believe might be a red herring to throw investigators off their trail. Deputy Chief Minister and Home Minister R.R. Patil stated that, if needed, the government would seek help of private IT experts to find the hackers.

4. Online credit card scam solved; three held guilty

A bank employee who had access to credit card details of the banks customers used them along with two other individuals to book tickets online and sell them to third parties. According to the information provided by the police, the scam was detected when one of the customers received an SMS alert for purchasing an airline ticket even though he had the card on him and had not used it. The alert customer immediately informed the bank who then involved the police. Eight days investigation by Cyber Cell head DCP Sunil Pulhari, PI Mohan Mohadikar, and A.P.I Kate resulted in the arrests of the three involved.

5. Murder solved with aid from MySpace

The murder of a high school football player was solved when police found the prime suspect in a picture posted on a street gang's MySpace page.

Whose law applies?

A hacker sitting in Iceland may use a proxy in Thailand to hack into servers of the London Stock Exchange. Which country's cyberlaws apply in this instance? The decentralized nature of the crime makes it that much tougher to demarcate jurisdiction, further compounded by that fact that cyberlaws are not consistent across nations (what may be a cybercrime in India may be perfectly legal in Sri Lanka).


For instance, the provisions of the Indian IT Act, 2000 applies, not only to the whole of India, but also to offences committed outside Indian territory, provided the offence involved a computer, computer system, or computer network located in India.

Where do we go from here?

Given the extreme pace at which internet users are increasing, the potential for cybercrime expands daily. Hence there can never be a perfect IT Act or cybercrime law which will cover all possible offences. IT laws need to be updated frequently, with more creative and inventive responses from



the organisations under threat. The laws and enforcement infrastructure also made aware to the general public. This also called for international co-ordination between enforcement agencies and shared jurisdictions wherever required. Piecemeal security solutions designed for individual threats are giving

way to strategically deployed systems aimed to counter multiple threats. Organisations should also consolidate their security mechanisms into a commonly managed appliance, instead of installing and maintaining disparate devices. These measures combined with greater user education are the best safeguard against the future of cyber-criminal activities. 

References

1. The Information Technology (Amendment) Act, 2008
http://www.naavi.org/ita_2008/index.htm
2. Types of Cyber Crimes & Cyber Law in India, Prashant Mali, CSIC (<http://dgit.in/WCyNDA>)
3. <http://www.cyberlawsindia.net/>
4. <http://dgit.in/UVeIT8>



OBSCENITY AND SLANDER: DON'T BREAK THE LAW UNKNOWINGLY

Simple things we do online may bring legal action your way. Read on and stay on the right side of the law

Complaining about the country's situation on Facebook and saying that XYZ politician is corrupt on Twitter is one thing. Being interrogated by police is totally another. Though both the things might not seem connected to each other, the fact is, they are. One of the points we hardly realize or take into account when posting content online are the laws. The most widespread idea is: "I have freedom of speech granted by the laws in the constitution". Another thought can come to mind in tandem with the first is: "Who is watching me anyway?" There are many other similar arguments that follow which help us convince that no matter what we do online we can just get away with it! Nothing can be far from the truth.

Being a responsible netizen in our time has become as important as being a responsible citizen. It is not the duty of our neighbour to warn us against online acts of profanity; it is our duty and responsibility to check those things. If only you remember the recent incident of the two girls being arrested by Mumbai police over a Facebook post, you would have realised how the online world isn't impervious real laws and how the body of law itself interprets online activities to punish offenders who don't toe the line. Of course in this case even the law was misused, but you get what we're trying to say.

It is notable that IT laws (or cyber laws) do not redefine everything. The fact is that they just define what actions taken online will be synonymous to what acts done offline. For example, if you are creating a public/open group on Facebook where you are sharing link to pirated software, then it would more or less translate into you teaching innocent people about how to loot a company building in the real world. Well, we can't tell you everything here because we do not have enough space and we're sure that the actual letter of the law does not excite most of us. So we will simplify things and put up a few guidelines, a list of dos and don'ts which you can follow to be safe online.

Every move we take online, every comment we post, every new status message, blog post, image upload everything is recorded, logged somewhere. Anything that appears publicly on this wild and largely uncontrolled medium of thought that is the internet can be tracked, if needed. The case of the Mumbai girls came into limelight due to the speed at which several steps were executed under a controversial situation. There is a possibility however, that actions could have been taken slowly and that the news would have never spurred the interest of masses the way it did.

What can be done online without getting into a legal trap?

Ask yourself - “what can be done offline (in real world, not on the Internet) to live a normal life without inviting into legal troubles?” The answer is obvious - you have to do your everyday job, live normally and make sure that you are not supporting any activity which causes disturbance to the harmony of society. Now, as complex as it gets with the Indian constitution, there are multiple laws protecting and governing any activity. Laws for online behaviour are not an exception either. No matter how confusing the pages of law become, there are simple ways to express it. If you are going to get involved into something heated and/or controversial concerning a topic which can be sensitive from any perspective (concerning topics that are religious, political, racist) then please go through the rule-books first. Except under some conditions, the following simple list should be sufficient to help you about what you can do online.

1. You may share your thoughts with the others. There is no harm in saying what you want to say as long as it is not about hurting a man's sentiments, or the man himself!
2. You can share pictures and videos with others because pictures and videos are means of communication of thought.

Just two points in the ‘dos’ list? Well, yes, because almost all others can be covered in the list of what not to do. After all, a lot of labour goes in the making of our online life; a lot of activities happen and we have got used-to a lot of stuff in a way that it is better to tell what not to do than about what to do.

What not to do online

Before we start talking about what not to do online, it is important to go back to the basics and remember that online laws more or less just define about what online activities would correspond to what real-world activities. Most of the “how much should the punishment be” part is handled by the traditional law. But once again, it is not required to go through a long manual unless needed. For our day-to-day life, the following list of suggestions should help you get along the electronic tides safe enough.

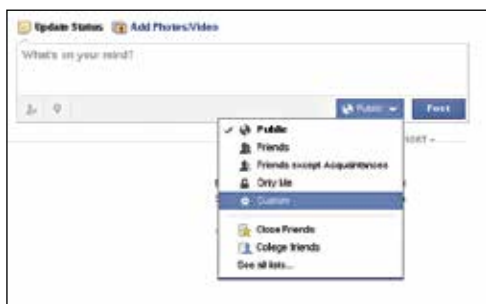
Don't get harsh

Always behave with-respect to people you know as well as to those whom you do not know. Slander will land you into trouble. At present, we live in a

society which does not take online talk too intensely and seriously. Someday, that would change though and perhaps very soon. If a person whom you insulted online files up a case against you in the court, you could be charged and punished accordingly as and when you are proved to be the culprit (and you will eventually be, if you did it). Remember that when you are online, communication with mere text which cannot carry any emotion or mood in which you write it. Articulation of your writing style is needed to suit the environment of the talk to make the text convey really what it means and yet, depending on the understanding of the language by someone who reads the same, it might appear objectionable. Hence we repeat: treat your online mates with respect.

Don't underestimate your audience's size or wits

When was the last time you changed the privacy settings of your post? Last month or last hour? And hey, when did you update your status last anyway? Do these things matter? Well, yes they do. If they did not, we would not be wasting ink and paper on it. Social networking sites have become a business place for the simple reason - wherever there are people talking, business blooms. The inflammatory post you make about your harsh boss be better not shared with your office colleagues unless you really trust them. Just like in real world, it is important to categorize your friends online. If you have



not, please do so now to avoid problems.

While you can have control over your friend list, you cannot have any control over the number, diversity and involvement of other people in a group. In such cases, your post or comment would be seen by a lot

Do care for who you share your thoughts with

of other people depending on the type of group it was made in, the strength of the group in terms of number of members and the randomness of the website's notification system. If any one of those who watched your post feel offended enough to file an official report against you with the police or in court, difficult times may follow.

Yet another factor which affects the reach of your post to another person is the 'share' feature available in different forms. On Facebook and Google+, you call it 'Share' and on Twitter, 'Retweet' would make up a synonym. If your post was public and anyone could share it, your voice becomes reachable to many (well, practically everyone). It is important that you just do not leave all your status updates open to public. If you do, you must make sure that you are not posting anything which can be used as a base for a legal action against yourself.

Don't be a social-network addict. Just be social

Posting nostalgic messages about missing your childhood and old games you played when you were a kid does not change the fact that you posted all of that online. The social network has made talking cheaper and easier to such an extent that we often forget to talk to our friends on phone or meet them personally. The lack of personal touch often results in even more attraction towards the social networks in hope of getting new friends, trying to gain attention of more people and avoid boredom. All of this leads to high levels of addiction which not only alter (and in many cases 'hamper') normal behaviour but can also lead to high depression levels.

Under such circumstances, it is easy to ignore the legal part of a world that still gets called as reality. Though it does not directly connect to cyber crime, depression caused by addictiveness towards online social networks is not very uncommon and play their role in enhancing the ignorance of a person towards the real world. Such ignorance can help propel conditions which lead to breach of law, online.

Don't disrespect women #Seriously

No, we are not going to talk about morality and why one should respect women. Sure there are moral reasons for the same but they don't really belong to this page. We just mean to convey that one should stay away from obscene behaviour towards any female online. You cannot track down all that you wrote, uploaded, and commented upon in the online world due to time constraints and limited search techniques available for such content. A single comment can lead you into a heap of troubles. Vulgar comments on any lady's pictures on a social media site is directly comparable to vulgar comments on a lady in real world and would be treated by law as such, accordingly.

There are facebook pages which share objectionable pictures of random girls over the internet. While some of those pages are focussed on well known public figures, there are some which just extract any picture they can get from other women's profiles and put them up for wild comments (you know what we mean, right?). Cease and desist.

Don't just upload any picture randomly

Facebook hosts more than a hundred billion pictures at this point of time and Gigabytes of images are being uploaded daily as well. Some of them are entertaining, some are serious, some contains messages. We are sure you too would have used the free service provided by the juggernaut called Facebook. Other services such as Google+, Twitter, Flickr, and Picasa web albums too are used for sharing pictures. So what can go wrong? Well, there are quite a number of things that can.

We have already talked about respecting women and we won't go explaining it all again but yes, posting objectionable pictures of women without their consent or cooperation can lead into trouble. We do not mean to say that you need to ask everyone before uploading pics of your birthday party, but to stay alert about not letting slip anything which can hurt the public image of a person. This not only applies to women but also to your friends of male gender.

One of the occasions when we take pictures in bulk happens to be when travelling. You are going out from your city for a weekend party or on a vacation to Kashmir, the one thing you are going to do is to take pictures. All across the country, there are quite a number of tourist places where taking pictures is prohibited. You would find regulations and restrictions about photography at a lot of



Refrain from taking pictures where it is not allowed

religious places for tourism or monuments of national heritage. Other places too can have such restrictions, such as inside a laboratory, or a museum. But we seldom follow rules, right? What difference does it make if we take that one picture? What if we just hide a camera in your back-pocket? Such things might not make a difference. But do you realize that sharing a picture which was prohibited from being taken can make a impact in your life?

The story does not end here about pictures because a picture can be of anything. Posting or sharing pictures of copyrighted material is a menace too. How many of us think twice before uploading the 'e-book' of a book online? Do we really care if the MP3 file we are sending/recieving online is a copyrighted property? Do we realize or remember or even care about the fact that copying content from Mashable and reposting them on another blog can cause copyright issues? Obviously we don't. Though piracy is rampant, we request you to stay clear of posting, uploading or sharing copyrighted picture online; unless you obtain prior permission.

We are not asking you to be paranoid about sharing pictures online. What we are asking you is, to wait for a moment before doing so, and in that moment and ask yourself whether or not the picture you are going to post or share violates someone's copyright or privacy and that the picture is of something which was not prohibited to be photographed. It is not required to keep a fat rulebook by your side. But do use a little common sense before posting pictures.

Do not get involved in hate groups

The internet provides a platform where good as well as bad things get shared real fast. There was a time we would have said that news spreads on social media like wildfire, but no more. Twitter is faster than earthquakes (<http://www.youtube.com/watch?v=OUFs7bYBxzY>) and a news can spread all around the world in few seconds.

All across the internet, there are groups and websites which are built to promote a particular idea or message. It is on those forums that you would find the maximum amount of hatred for the polar opposite idea. For example, if there is a discussion forum dedicated to Windows 8, there are chances that some members on that forum truly dislike the Mac operating system. Though we have given a very lukewarm example of hatred which cannot be stretched too far to cause any harsh legal actions, there are many other hot topics that can lead to heated debates and escalate out of control.

The internet can act as a platform to spread false claims and misleading, uncited information and there are examples aplenty. Before condemning Shahjahan on his practices in his time or Bill Gates on his software, make sure that you have enough credible proof to say so. While Mr. Emperor is not going to rise back from the dead, the other guy we just mentioned is still alive. Well yes, he does not seem to care much about what the world has to talk about him, you do not want to condemn reputable people based on incorrect information, do you? That's just plain embarrassing.

When discussing controversial topics online which involve people, places or actions, it is advisable to stay away from blind criticism. Such criticism is often sourced from hatred and breed the same. Quite a number of times, as it happens, hateful messages is based on false assumptions and misleading information gathered from unreliable sources. One of such examples is a post which was floating around on Facebook where Bill Gates was said to be son of a farmer which is not the case (check reputed sources). We recommend you disconnect yourself from groups which spread false information. If disconnection from the group is not possible, you must keep your cool and stay as far away from heated and baseless discussions as much as possible unless you have proof to back up your arguments and more importantly, a reason to speak. Replies intermingle and confusion grows. Stopping yourself from continuing your involvement in such discussions is the best way to avoid the thought of "calming others down and putting them on the right track" which only heats up topics for no reason. It is also advisable that you anticipate the result of your actions keeping the law in mind. We repeat - make sure you have enough proof from reliable sources before commenting on any person's social stature.

No prejudice about hiding your identity

There are people on social media and then there are 'fake people'. These 'fake people' are the real people using an account which impersonates someone. But then, is a fake profile really anonymous? Well, no, not really.

It is not uncommon to come across situations where a fake account is being used to get out a piece of information from another person using social engineering tactics. The practice is especially prevalent among teenagers. Often, the motivation for most of these fake profiles is fun and playing pranks with friends, but things can get ugly down the line. The sense of anonymity that a fake online profile provides increases as a person keeps using it. The user can end up using it for unlawful purposes such as sending

threatening emails and harassing others. Though he might think that he is invisible, that is not really the case.

Nearly every online activity is logged somewhere and not everything you delete gets deleted. If required the authorities can procure the required information from different companies whose services you use. Your location and where you were at a particular point of time can be found out using your cell phone's location or IP address. With constantly improving face detection technologies, your face can be spotted in other people's pictures too (did you think about that one?). Your call history, email history, private conversations everything can be extracted once the government wants it all and as long as things are logged (and believe us, almost everything gets logged). Online anonymity is nowhere close to truth. Though there are methods to avoid being caught, these methods are too technical and advanced for a day-to-day use and yet they are not guaranteed to hide you well enough. Again, most of those methods are not legal. If you have got any trace of the 'online anonymity' idea in your head, please get over it; there is no such thing in our most day to day online activity.

Though these were the guidelines, it is important to realize that online or offline, every move we take is under surveillance and possibility of being questioned remains open. Try not to be unlawful when enjoying time in

Bill Gates went to a restaurant and paid a \$2 tip. Waiter said "Yesterday your son gave a \$100 tip and you are giving only \$2?"

Wise reply by Bill Gates "He's the son of a billionaire I'm the son of a farmer."


1,402 people like this. Be the first of your friends.


0

[Like this app?? Become a fan!](#)

Gates was born in [Seattle](#), Washington, to [William H. Gates, Sr.](#) and [Mary Maxwell Gates](#). His parents are of English, [German](#), and Scots-Irish descent.^{[13][14]} His father was a prominent lawyer, and his mother served on the board of directors for [First Interstate BancSystem](#) and the [United Way](#). Gates's maternal grandfather was J. W. Maxwell, a national bank president. Gates has one elder sister, [Kristi](#) ([Kristianne](#)), and one younger sister, [Libby](#). He was the fourth of his name in his family, but was known as William Gates III or "[Trey](#)" because his father had the "II" suffix.^[15] Early on in his life, Gates's parents had a law career in mind for him.^[16] When Gates was young, his family regularly attended a [Congregational church](#).^{[17][18][19]}

Do not just trust anything on the internet said by a random person. Research before you move along

front of your computer screen. Most of the time, using your intuitive sense of righteousness is good enough. Avoid being involved in acts of slander, obscenity and baseless discussions over matters that are beyond your control and try not to accuse anyone for something unless you have solid proof. If you feel that you want to take an online step against something to make a change, please get genuine proof to back yourself up and go through the rules. If in doubt, contact a lawyer who deals with online laws. For your reference though, we provide below the links to the IT act 2000 and IT amendment act 2008

- ▶ IT act 2000: <http://eprocure.gov.in/cppp/sites/default/files/eproc/itact2000.pdf>
- ▶ IT amendment act 2008: http://deity.gov.in/sites/upload_files/dit/files/downloads/itact2000/it_amendment_act2008.pdf 



CYBER TERRORISM

From your monitor to the valley of fear:
Find out about the changing face of
terrorism in the age of technology

Every religion in the world has taught us since centuries to treat our fellow humans, even enemies, with love, for love transforms. But how do you treat someone with love when he intimidates and hurts you, drive your world into chaos and you don't even know who he is. How would you protect yourself from someone whom you don't know and can't see? Quoting Ra's al Ghul from the movie *Batman Begins*: "Men fear most what they cannot see." Welcome to the world of faceless terrorism.

But, but...it doesn't exist

What if we told you that this anonymous terrorist doesn't even exist? What if we said that the very word "cyber-terrorism" is a completely made-up term and you didn't have to worry about a thing? Would that make you happy? Would you consider this chapter useless? Well, sorry to burst your bubble but it's very real. Maybe you'll find solace in the fact that there are more than a handful of naysayers who are in complete denial over cyber-terrorism's existence.

Cyber-terrorism has several definitions which range from very narrow to very wide. The definitions vary from virus attack threats on targeted personal computers (the narrow definition) to bringing down a large network and disrupting everyday activities (the broad definition). These of course are very broad and very narrow definitions. Basically cyber-terrorism takes root when terrorist groups exploit the internet to carry out attacks on their target enemies.

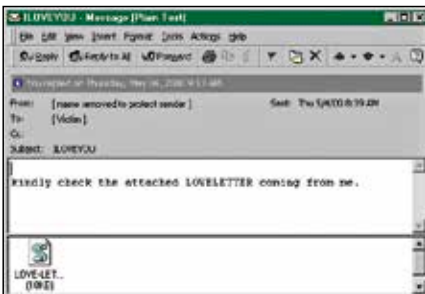
The narrow definition

From a narrow viewpoint, cyber-terrorism means hacking and information warfare which involves targeting computers and their owners and threatening disruption of infrastructure and physical harm to people or property. Although there haven't been any significant incidents of such a type of cyber terrorism, there has been concern about its occurrence, especially due to movie watchers being inspired by the likes of Live Free and Die Hard which include examples of both, narrow as well as broad definitions of cyber-terrorism.

Since cyber-terrorism as per this definition involves targeting and hacking individual PCs, cynics reject the theory of cyber terrorism based on the fact

that an attack on computer networks is very unlikely to be a source of terror, fear or significant number of deaths. Since the amount of harm is restricted, they cite it inappropriate to call an electronic mayhem an act of terrorism.

This viewpoint can't be challenged since there



Love bug caused problems in the wild

haven't been any major activities in the past which directly damaged property or lives using electronic methods. What strengthens the argument is the claim by most researchers and companies that the computer systems and networks of today are safe enough to counter widespread denial of service on everyday activities.

The possibilities

While the narrow definition of cyber-terrorism is not wrong given that any widespread disruption in services hasn't been encountered, possibilities still linger. A simple look around would reveal the chances. Let's consider a day-to-day life of an imaginary middle-class person named Yash. Later using the same example, we'll show you how dependent we've become on computing systems.

1. It's 5:30 a.m. and Yash's alarm on his mobile phone goes off. He slides the icon on his smartphone to turn it off and wakes up.
2. After freshening up, he grabs his laptop to check for any important email from the office or messages from friends. He doesn't find anything significant; only routine email from his work colleagues. Regular stuff. All is well.
3. Yash showers, dresses and leaves for work on his bike at 9:25 a.m. He reaches office in 45 minutes at 10:10 a.m. Thanks to the extra traffic and red signals at the most inopportune of moments, he's late. Not much of a problem; he escaped a telling off since even his boss is late!



Though not terrorism, BJP party site defaced by Anonymous as part of a co-ordinated attack

4. The bank where Yash works teems with customers for the complete duration of the working hours. Since Yash is a bank teller, he handles their cash deposits and withdrawals.
5. At 6:00 p.m. he logs off his computer, finishes some other work in his office and is ready to leave for home at the normal time.
6. He leaves at 8:00 p.m. and reaches his room at 9. Takes his dinner, passes some time with his laptop, talks to friends on phone and goes to sleep.

Now how is cyber-terrorism supposed to harm our man? Let's go over his schedule and see how he was stuck at a computer all day, in the same order as his day passed.



Airtel network down due to technical difficulties

The guy wakes up to his mobile phone alarm. These phones feature large app markets with various apps. A directed cyber terrorism attack can cause a virus to spread through the marketplace itself,

disrupting our protagonist's life right from the moment he wakes up. As the day progresses Yash will take his car to work. If the computer controlling the traffic light made a mistake of switching on the green light before actually putting up a red signal for the other direction, Yash could potentially meet with an untimely demise.

Yash works in a bank and banks work on internet (yes, they work on intranets and VPNs most of the times but they connect to the core system using the internet). If his computer was infected with a new virus which was specifically made for the application he uses to handle transactions, he could have been doomed if the virus caused losses to the bank or the customer. .

In our everyday life today, we encounter technology at every single step. From the intelligent 'microprocessor controlled' bikes to cars with augmented reality, from the doors of metro rails and traffic lights to air traffic control systems, from mobile recharges and ATM machines to online money transfers - technology is everywhere and we are dependent on a lot of such stuff every day.

What if a lot more services were brought down in one go? What if mobile phone networks of not just one service provider but multiple ones were down? What if the traffic control system of an entire city was down? What if all apps in Google Play store were infected with some bug? What if a new virus attacks and a lot of data is destroyed? You being a reader of Digit raises the probability that you know of stuxnet. What if something very similar hits all manufacturing systems and assembly lines go haywire? Already sounds like apocalypse? Well, it could be worse given the fact that we are all so dependent on computational systems already.

Fret not, the chances that all such things happen on a single day is pretty rare.

How bad can cyber-terrorism really be?

We started off with a narrow definition of targeting a small number of computers either specifically or randomly and went on broadening our imagination up till the effects of cyber terrorism activities could cause a mess huge enough to spark uncontrollable level of violence on streets. Most people are either in denial or disagree with the premise that cyber terrorism activities could surmount to a level that could possibly cause physical damage. One of the arguments that they can use to back themselves up is: "Who is going to do that?" We try to answer that question here.

Putting a range of computers on target is not a big deal. A single malicious hacker with the right tools, information and skill could do that. If the range were to be larger, the number of people behind the act ought to increase as well. This would be because a single person would not be able to take down large systems on his own due to time and resource constraints. We've already presented to you the scenario depicted in the movie *Live Free or Die Hard* but a movie is based on a number of assumptions. Though philosophical, the fight of good and evil is eternal without computing domain being an exception. Experts have said ever since that no system is perfectly safe and we have learnt to live with that. Incidents of breach take place everyday at various levels and the systems we work with, software, operating systems, networks and protocols are all vulnerable at some point. However, systems that we depend on, are heterogeneous - different operating systems, versions, update patches, network components, their software versions and updates and specific application vulnerabilities together pose a wide array of possibilities. From a hacker's viewpoint, as you go on increasing the number of target systems, you are going to need more hands and skilled brains.

If we are to consider two mobile phone networks, not only the entire software set but also the overall networking methodologies might differ. So an attack method on one network does not guarantee that the same is going to work for another as well. So in effect diversity results in division of risk.

So we can vaguely answer the question of “Who would do that?” as “Multiple teams of skilled hackers”. Let’s move onto next point: the timing. The situation we imagined to backup the broad definition of Cyber-terrorism involves two or more systems going down at once. The new question is “Is it possible to take down two systems at once?” The answer to that question too would be ambiguous and difficult to answer in a plain yes or no.

Critical systems are protected by critical countermeasures developed by highly skilled professionals and experts. Chances to break through them are very low. If a security loophole is found out by a (team of) hacker(s), then the possibilities of exploitation of the loophole depend on the ethics of the hacker. If it was an ethical hacker, he would notify the system administra-



The movie Live Free or Die Hard is one of the best depictions of the broad definition of cyber-terrorism

tors. Also, maintainers of critical systems usually have a separate team for vulnerability testing which keeps attacking the system (with legal permission from the company) to test if it system could be attacked. If the hacker who found a way through was malicious, there are again two possibilities: i) He could create program(s) to exploit the vulnerability OR ii) coordinate with other hackers who already have found a bug in another critical system to launch a parallel attack on both of them.


Look back and you have certain conditions governing the possibility of takedown of two systems:

- ▶ Security research teams did not find a loophole.

- ▶ Two individual hackers or teams/groups of hackers found vulnerabilities in different systems at the same time.
- ▶ Both the groups had malicious intent.
- ▶ Both hacker groups knew about each other and communicated with each other for the plan to attack.
- ▶ None of them launched the attack on individual basis.

Even if one of the conditions did not match two systems cannot be brought down at the same time. Add to this mix the fact that various companies involved in providing the hardware and software which constitute such systems keep researching on their ends as well.

This boils down the effects of cyber-terrorism to its bare bones - the narrow definition which includes the use of viruses and other malware. The target can be either random or specific group of computers. In most cases the viruses are spread out in the wild which makes the target random. Antivirus companies are at work to counter those and virus attacks in general have always been prevented until now. Additionally Microsoft has been working on its end too to provide more security to its users. We cannot talk about Mac and Linux for there hardly are any viruses for them and the fact that they constitute very small percentage of computer users makes them a weak spot for being targeted by cyber-terrorists (or hackers). Thus, in the public domain the cyber-terrorism has less chances to happen as well.

Let's summarize this entire chapter. We started off with the broadest definition possible for cyber terrorism. Then we introduced to you the narrow definition and widened our view towards what could happen in the name cyber terrorism area and yet again cancelled the possibilities of each one of them. What conclusion can be drawn in the end? Well, the fact is - the narrow definition of mere use of viruses and malware does exist to a fair extent but cannot be labelled as 'terrorism' in its own right as it cannot cause a havoc. However, beyond that point, there are possibilities and those cannot be denied. Though there have not been many cases of attacks on critical networks, there are chances. There have been events of takedown and website defacements to spark off wild imaginations of computers being responsible for a widespread mayhem. The case we left off was "targeting specific group of computers intentionally for attack" which we would cover in the next chapter as they are not acts of 'terrorism', but of 'war' by one group on another. 



CYBER WARFARE

Find out how the wars of the future are going to play out... In cyberspace

Byline: "Some men just want to watch the world burn"

– Alfred Pennyworth (The Dark Knight).

Before we go further, here is what Wikipedia says about cyber warfare:
"Cyberwarfare refers to politically motivated hacking to conduct sabotage and espionage. It is a form of information warfare sometimes seen as analogous to conventional warfare although this analogy is controversial for both its accuracy and its political motivation."

Cyber warfare might not be the biggest news as of now, but there has been speculation, based on reported incidents, that it has been performed in the past and that it will only grow in days to come.

Humans haven't been much of a kind species. Wars have been fought since forever. Weapons have changed, however, from bows-and-arrows to ballistic missiles. Today, cyber weapons are increasingly becoming the new frontier of war. As the use of computers increases in the daily life of people and more and more things start getting controlled by computers, information warfare is going to rise.

We have already talked about possibilities in the previous chapter about how an attack on critical systems could disturb day to day life and all of a sudden, convert mundane activities like 'talking to someone on the phone' into a next-to-impossible task. But what we talked about in the last chapter was not about warfare, it was about terrorism, terrorism caused using computers. Cyber warfare actually means 'war' and is as much serious as a war would be.

Motivations behind Cyber Warfare and potential threats

Though wikipedia says that Cyber warfare is politically motivated, it is not the only case. There may be other reasons too because a war is a war; who is attacking whom and for what reason is not included in the meaning of the word.

Political and Military motivation of Gathering Sensitive Data

Political reasons are one of the most ancient reasons for war and like we said, only weapons have changed. There have been numerous incidents which suggest that weaknesses in computing framework used for management of a nation can be used to gain significant advantage over a country.

Sensitive national data is handled using computers and they are connected to the Internet most of the time. The data might include a country's financial database and history, military research and plans



CBI website has been hacked in the past as well!

and other governance related data. A compromise of servers containing sensitive data (especially military data) can make a huge impact on the future of this planet depending on what information was extracted from where and when. Control over weapon deployment systems could finish a war even before it started by using the weapons designed by a country against itself. Control over large weapon systems such as missiles may lead to catastrophic results.

The possibilities do not end here. If the hackers who penetrate systems with critical data might be able to change the data as well, it could result in change of long term plans and mislead entire operations into traps. Deleting data can cause complete disorganization and void plans. Under high stress conditions, this can prove fatal to a significant portion of the world's population.

Motivation to Sabotage Civil Life

When critical systems get connected to a common central network, the possibility of bringing them down becomes easier than it would have been otherwise. Electricity is at the heart of what we do in our day to day life. Bringing an electrical grid offline can cause massive service disruption as all other information infrastructure depends on electricity. There have been known attacks on US electrical power grids already. (<http://news.bbc.co.uk/2/hi/technology/7990997.stm>). In case the power grid is nuclear, an attack on the control systems can potentially convert the power source into a nuclear bomb (once again depending on what depth the hack went to).

Electrical grids are not the only targets in cyber warfare. Other resources such as public transportation, communication, water and fuel are also increasingly being monitored and controlled using computing systems for the sake of automation. A successful attack on any of these can open a gate of immense troubles which can potentially bring a country to a standstill, as we have already discussed in the Cyberterrorism chapter.

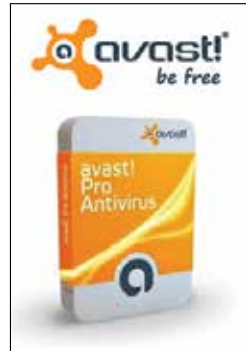
Financial Motivation - harming the competition

Bots such as stuxnet which can manipulate manufacturing processes of other equipments by hacking the logic of a PLC (Programmable Logic Chip, used in automation of assembly lines) pose a huge threat to the manufacturing processes of various equipments. An attack on manufacturing units and factories can cause huge losses to a nation too, not to mention the company which owns the factory. And we did not even count using

cyber attacks (hacking attempts) as potential weapons to cause harm to competition. All of this combined can harm the economy of a nation really hard. Financial motivation is one factor which crosses boundaries by all means. The competition may be between two companies belonging to two different nations or even the same nation.

Strategies and tactics for Cyber Warfare

The cyber dimension of any conflict has till now existed behind the curtain. The approach of hiding the attack is also what gives cyber warfare a significant part of its power. Hence, one of the prime objectives of a cyber warrior (we hope we did not term the hacker wrong) is to remain anonymous.



Antivirus is one of the most vital software needed in the interconnected world

Anonymity

One of the most trusted methods used by clever hackers for maintaining anonymity is to route the attack via other computers. The number of computers used for routing the attack can vary but in most cases at least two are involved. This technique is called 'hopping'. The selection of computers that are to be used for attack routing is done based on the diplomatic relationships of the target country (the country in which the target computer is located) and the routing country (the country in which a computer to be used for a hop is located). If the diplomatic relationships between the target country are not good with the routing country then the investigation of the attack would be more difficult due to non-cooperative stance that would be shown by the routing country. If there are more than one routing countries involved, the situation gets worse because the target country would have to negotiate with yet another non-cooperating country. The open nature of the Internet can be used as a protective layer for the identification of the source of attack. If the cyber attack was sponsored by the attacking country, the investigation can be completely defeated by complete non-cooperation by the attacking country.

Cyber Laws and International nature of the Internet

Though there are laws dealing with cyberspace, they may not be enough

to counter a large scale targeted attack. In addition, traditional law enforcement techniques, and their expertise, are not of much use on the internet where identities can be easily faked and levels of anonymity are high. This requires that special methods be devised for the internet and a new and special set of officials are appointed to monitor the same. Moreover, the internet is not limited to any country. Making sure that you have the best men, machinery and laws for dealing with an attack does not mean that you will be able to prevent it.

DoS and DDoS - Brute Force, Network Style

Cyber Warfare is usually done by targeting systems which are very important to support critical infrastructure. While hacking into the system is the preferred way to get information from the system, there is no guarantee that this would work - the people who run the systems and the ones who attempt the hack on them are often on not-so-distant levels of intellect, coordination, speed and efficiency. In cases when it is very difficult to figure out a way to infiltrate into the system, there still remains a method using which the system could be made useless for the original purpose, called a DoS (Denial of Service) attack. While it is more of a 'side-way' of attack at times, there can be situations when DoS is used as the first method of attack. Such an approach is used due to the fact that as long as a system can be reached over the network, DoS is bound to bring the system down.

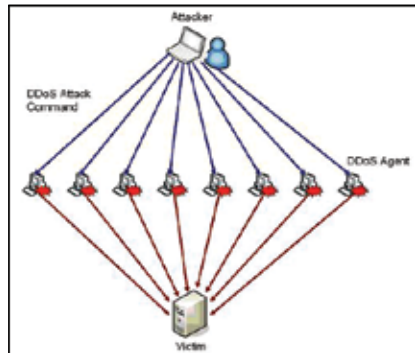
There are a lot of ways DoS can be implemented. While some of them work on the patterns of port scan, higher level (usually application layer) attacks can also be used depending on the type of system being attacked. DoS involves flooding the target computer with requests (e.g. making too many requests for a web page to a web server). When there are a lot of requests coming in, the target computer is bound to fail trying to serve all requests at some point of time. But this does not work all the way for everything. Take for example Facebook - one of the busiest websites in this world. It is said

NOTE

Although wars have always been fought between countries, the evolution of the Internet has changed things. Cyber warfare is not done only between countries. Today, it can be started off between any two groups on the internet. The fact that the groups can be widespread all over the internet makes it much more difficult to contain than the normal outbreaks between groups in the real world.

that during peak traffic time, Facebook processes more than 500K (that's 5 lakhs) requests per second. Sending it a few more thousand requests per second would not make a lot of difference. For such cases, there is another, more dangerous method: DDoS.

DDoS or Distributed DoS is the power of DoS multiplied n number of times. The number n is the number of



DDoS - Brute Force attack, the networking style

computers involved in DoS. Confused? Well, DDoS distributes the overall DoS load onto multiple computers which parallelizes the effort and multiplies it. We can think of it like this: If 5K requests to Facebook do not bring the servers down, let us get 1000 computers and make each of them fire 5K requests to Facebook servers per second. In such a case, you would be sending $5000 \times 1000 = 5,000,000$ requests per second. Now, that might just bring down Facebook if its servers cannot take that many requests! The toughest part of DDoS is simply getting that many computers.

In many cases DDoS is performed by an army of Zombie computers which are already under control. These computers may be anything from a smartphone to a server as long as they are connected to the internet and can be commanded to send huge number of requests per second. To create such an army, yet another step comes in - to create a virus which can be used for creating backdoors for commanding, controlling and/or scheduling the DDoS attack. However, since cyber warfare is usually pre-planned by a group, the availability of computers may not be a problem.

One of the biggest strengths of DDoS is that not only can it flood the servers, it can also bring networking equipment to a halt. Typically, when DoS is detected (well, there are systems for that too), networking equipments are configured to block any requests coming from the attacking IP address. If there are a few computers located on the same network which are attacking the target, a blocking rule can be set on a complete IP address range. As the number of computers increase along with the diversity of IP addresses which are being used by the sources (computers) of attack, the rules get more complex. Let us consider the previous example of attacking Facebook servers:

If one were to send a total of 5 million requests per second to the servers, the total number of incoming requests will rise to 5.5 million with 10/11ths of the traffic being useless. If the network equipment at Facebook is configured to drop the requests coming from attacking computers, it would probably still overflow the capacity of the equipment to handle traffic. This might result in packet loss of genuine requests and thus disable the services. And then, not all websites can handle the amount of traffic that Facebook can!

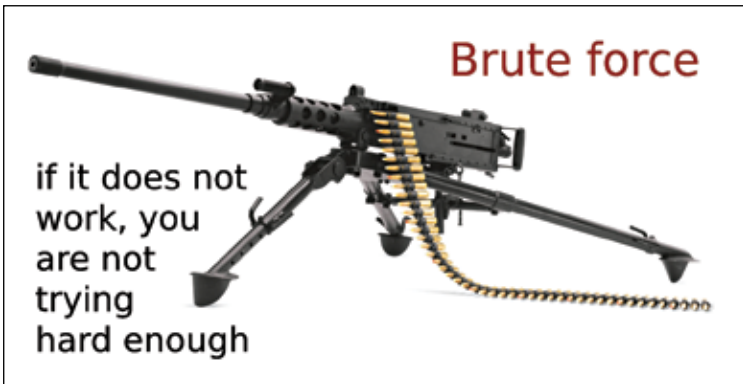
It is important to know why DDoS is one of the biggest weapons that can be used in cyber warfare. The only protection which can be implemented to prevent DDoS from happening is to close the access to the systems from the outer world, i.e. to prevent the access to the system (we are talking about critical systems here) via the Internet and that as such is a very difficult scenario given today's interconnected world.

'Speaking in Gibberish' is important

One of the prime reasons critical networks cannot be run on a separate network is the geographic area and costs involved. Take India for example. The distance between Bangalore and Delhi is about 2000 kilometers. If one critical system were to be located in Delhi and another in Bangalore, more than 2000 KM of networking infrastructure would be needed to interconnect them. Though security is a prime requirement for important computing infrastructure, the costs cannot be neglected. Relying on the Internet not only makes more sense but also saves money.

Now comes the tough part. Communication between any two critical systems when done over the Internet, faces the possibility of interception i.e. data being copied over the wire. This can be done by compromising any of the networking equipment involved in the transfer of data - cryptography comes into the picture (we hope you did go through last month's FastTrack on cryptography).

Though most important data is transferred securely, a mistake can cause the information to leak out into the wild. In addition, weak cryptographic methods can pose a serious threat to the security of sensitive data. The point worth focussing on is the 'weakness' of the algorithm. We already know the security of algorithms depends on two factors: strength of the algorithm and strength of the key. Years of research has yielded quite a number of secure algorithms such as RSA (one of the most famous ones). The part which still remains challengeable is the strength of the key. The only known method to break such algorithms is brute force.



A brute-force attack is guaranteed to break a cipher eventually

Under normal circumstances, breaking a public key cipher via brute force might take a lot of time. But cyber warfare is rarely a normal situation. If an attack is conducted by a very large organization or a country, it is possible that they have enough computing infrastructure that they can attempt a brute force on medium-level security. In case of nation sponsored attacks, it is possible to include mathematical research and expertise to aid the brute force.

Role of Computing hardware in breaking ciphers: If you think the processor in a normal PC can break a cipher using brute force that governments might be using, then you are not wrong, not at least technically. Normal processors available in market can be used to break ciphers quite well however, they are not good enough to do it within limited (read useful) time period. This is because the CPU is designed to perform parallel processing only to a certain degree.

GPGPU technologies such as CUDA, OpenCL and DirectCompute can be used to accelerate the process by thousands of times. If one is to take the help of advanced databases and previous research done in the field, the process can run upto a million times faster. If you dive into the architectures of some of the top supercomputers of this day, you will find GPUs in use. The current fastest supercomputer Titan uses GPUs from both the red and green groups (we mean AMD/ATi and Nvidia). That does not mean that it is all insecure. Strength of a cipher usually increases exponentially with linear increase in strength of keys. Most communication is done using strong enough keys and it is still difficult to fetch your Gmail password

from over the wire; RSA 2048 is a long story anyway.

Prevention is better than cure

What can you do?

To avert invasion is always more difficult than to avoid it. But what can a normal user like you and me do? Well, basically nothing except prevent ignorance. Allow us to explain that sentence again. One of the biggest attack methods that can be used against any system connected to a network is DDoS.

Since DDoS requires a zombie computer army, the first measure you can take is to protect your computer from being zombified. If someone sitting remotely can control your computer then it is certainly bad news for you. There are a lot of other problems but from the cyber warfare viewpoint, your computer could be used for attacking another computer. If the target system is not built for very high traffic, then less than a dozen computers can be used in a DoS attack. Once again the international nature of the Internet can work against you. For e.g. if someone sitting in a foreign country takes control of your computer and uses it to launch DoS/DDoS attack on one of the critical servers of your own country, you can get into a lot of trouble.

At the same time, it is important for the employees working in government offices to protect their computers and laptops, especially for those who work with critical information. A lethargic approach to security by them can create backdoors to critical national data.

What can Governments do?

The first and foremost job that Governments can do is to create policies about the actions and steps to be taken when a cyber attack is detected. The second step that can be taken is to ensure that the ISPs throughout the country follow specific rules which can suppress attack methods like DDoS. Also, wherever possibilities exist, a separate and more secure network should be used for communication between two systems dealing with




Nvidia CUDA helps accelerate applications with heavy instruction-level parallelism requirements and is available on most NVidia graphics cards in the market

important national data. Not only this, they must implement guidelines for government employees to make sure that the nation does not pay the price for their mistakes. A reassessment of the quality of security professionals to counter the latest techniques of cyber warfare is also needed.

A word on Open Source

The biggest advantage of Open Source is, well, openness. In most cases it is also free of cost. The open nature of open source makes sure that it is available for modification by anyone who uses it. Since the program is modifiable, special modifications can ensure security at lower levels of data access e.g. embedding security within the modules which deal with network protocols or creating a new file system (or modify an existing one) which encrypts all data before writing to disk. While these are very small examples, a lot more sophisticated methods can ensure that entire systems are protected by default and that mistakes by employees on their personal computers or office workstations do not end up opening a backdoor of any kind that leads to an information leak or interception by a third party.

Deployment of open source technologies also makes sure that an internal team could be maintained to take care of any vulnerabilities rather than depending on the software vendor to do the task. Not only this, since national infrastructure cannot be built using a handful of computers, open source can help save a lot of investments in software as well. 



STAY SAFE ON THE INTERNET

Safety tips for end users in IT dealings.
These simple things can keep you safe

Let's admit it. Our lives revolve around the internet – paying utility bills, booking movie tickets, shopping for anything and everything, getting married, finding love and even, making a social impact. But with cybercrimes like phishing and data theft on the rise, it pays to be safe than sorry.

What is cybercrime?

Before we delve into the safety measures, it is important to know about the different types of cybercrime, to effectively implement prevention

methods. A crime that is committed or facilitated by the internet falls under the definition of cybercrime. It can be anything from spam mails to fraud attempts. Cybercrime can also mean the unauthorized access to government or corporate secrets through criminal methods. Interestingly, cybercrime also includes illegal music downloads.

Non-money activity on the internet also accounts for cybercrime. For instance, creating viruses on other computers or posting confidential business information on the World Wide Web. There are many categories since the internet is vast. A complete knowledge of the different types of internet fraud would actually help circumvent the danger.

The key to staying safe on the internet is by understanding the fact that protection of personal and private data is absolutely important. And, in our world of Facebook and Twitter, this could be a tough task. Any internet related activity is vulnerable to crime and can lead to victimization, which can be traumatic. Sadly, the tools used are a lot more complicated resulting in a plethora of crimes on the internet, not really good news for the end users. The complexity arises due to the ability of the internet to provide anonymity to the criminals and offering them a range of victims who can easily be conned. So, in perspective, it is the responsibility of the individual to protect not just themselves but also their families from internet crimes. This can be done by ensuring safe online practices which will be highlighted in detail in the following pages.

Parental guidance

A lot of cybercrimes revolve around unsuspecting teenagers and school children. Parents play a vital role in ensuring that their children are safe on the internet and not vulnerable to hackers and identity theft. To start with, treat confidential information as confidential. Never reveal such sensitive data on the internet. Begin by telling your children that giving out personal information like address or telephone number or Facebook password to friends, on or off the internet. Ensure that your children don't do that as vital information should be kept secret.

It is always better to have a strong firewall installed in your computer, especially armed with parental controls. You can choose from commercial online services which offer amazing features, letting you and your child be safe.

Teenagers have a complicated life and an internet prowler sure is not going to make it any easier. Ensure that your children don't agree to meet

any “online friends” made through social networking sites. If they do, make sure that they discuss with you and go ahead with your permission. If such a thing should happen, choose a public place for meeting the “cyber friend” especially in the presence of an adult.

A lot of language on the internet is bad and if your child gets a particularly obscenely worded message, advise them to not revert. This also applies to those messages which are creepy or just plain weird.

Another rule on the internet, especially for the youngsters, is to never send out their photographs to any of their cyber-friends. Most often, such requests usually harbour ill intentions and can compromise the safety of your child.

Ensure that your children know that they must never enter an area where they are charged for services without being asked.

Interact with other parents and keep in touch with the latest threat on the internet. In our world of instant information, ignorance is sadly, not bliss.

Also ensure that the internet access to children, at home or school, is closely monitored by a responsible adult.

The ABC of internet use

Always be careful each time you are on the internet. Never write down your passwords. Memorize them. This rule also applies to other sensitive information – like social security number or credit card information.

First step – keep your computer updated. Switch off auto updates as most cybercriminals use such flaws in computer systems to attack your machine while safely remaining anonymous. The simple act of not opting for auto updates can cut down a large number of automated attacks on your system.

Ensure that your computer comes with a secure configuration. This simply means having to walk that thin line between too much or no security. If there is too much security, there are chances that the user gets frustrated. On the other hand, no security means increased vulnerability to cybercrimes. Most computers can easily be configured to provide maximum security.

Choose passwords that are strong and protect it. Your username, passwords and personal identification numbers (PIN) are quintessential for each and every online transaction. A strong password should be an alphanumeric melange and should never have the obvious details, like your name or telephone number in it. Using the same passwords for many sites increases

the risk of exploitation caused by discovery of your password. Ensure that you change your password every 3 months.

Your firewall keeps your system safe and secure. Keep it turned on always. This helps protect your system from hackers who might be interested in stealing data and crashing your system. Single computers especially require strong firewalls. The firewall software can be easily purchased for individual systems and for multiple networked systems, hardware routers double up as firewalls. And make sure that your firewall or antivirus software is updated and equipped to prevent malicious attacks on your computer. The antivirus scan must be done regularly and should come with enough capacity to remove the malware, if any.

Viruses can infect any computer without the user's knowledge. Since most antivirus software can update automatically, the risk is considerably reduced with the help of a strong antivirus. Most computers come along with some form of antivirus already installed. This just reiterates the importance of having a dynamic antivirus installed in your system. If you don't have it yet, do it now. NOW.

Don't fall for phishing

One of the most common forms of cybercrime, phishing is where criminals send fake email to the user, pretending to be a bank or a credit card

provider. Phishing is on the rise and is perhaps the largest form of identity theft in the internet. Luckily, the banks are now aware and are sending emails to their customers, warning them of phishing attacks and creating awareness among the general public.

Phishing approaches unwary users, most often persuading them to part with their confidential

information, including details like credit card PIN and online banking passwords. These happen on websites that are cleverly deceptive and are replicas of original websites of banks. Sadly, phishing is now a global menace,



with complex international gangs plying their mechanisms in intricately devious ways. And phishing is one of the highly successful cybercrimes, prompting banks to create awareness and cybercrime units to carry out intensive investigations.

While customers get wary of internet banking, phishing attacks are becoming more complex and highly ingenious. While earlier phishing attempts require users to visit the website, the more modern ones have an embedded link in the mail. Accidental clicking on these can lead to disastrous results – the download of a Trojan virus monitoring the user's surfing activity, giving easy access to cybercriminals. Some attacks may be put together sloppily and come across as fraudulent but others are highly sophisticated. Worse, this is conducted invisibly and users don't realise the risk they run until too late. However, there are ways to stay safe from phishing.

Avoid websites which are suspicious and be careful with emails from any company requesting for personal or financial information. On a similar vein, don't ever click a link in a mail, even if you have the mildest suspicion of the sites authenticity.

Similarly, type out the URL of your bank rather than clicking links. And before you start, check if the website you are visit is secure. Easy way to do this is by looking out for the padlock sign on the browser's toolbar. This means that the site which you are visiting is secure.

Change with the times

Never open attachments in your mail, unless you are sure of the sender very well.

Before logging in, check if your browser is updated, especially with relevant security patches. For Internet Explorer browsers, there is a special plug in to block out certain phishing attempts. Other browsers like Firefox or Opera are safer than IE.

It also is a good idea to use a personal firewall, equipped with anti-phishing toolbars that can immediately inform you if a phishing site comes along. Similar software can also be used to remove spyware.

Many users have the habit of storing information of their account on files in the system. This can be dangerous. But more importantly, be aware of internet fraud and also cultivate judiciousness to fake emails.

Read up on phishing and arm yourself with the latest updates. For instance, a lot of phishing attempts emerge as a plea for donations, espe-

cially after a natural disaster. Not really cool, whichever way you look at it. There are many websites which exclusively offer free education about fraudulent attempts on the internet. The Anti-Phishing Working Group offers information and the latest reports on attacks.

Many email providers have an option that lets you report suspicious emails and phishing scams. Reporting such incidences can help prevent receiving more such emails; especially with the abuse team working extra hard to stop similar attempts in the future.

Most scams are usually alarming messages which threaten of account closure. Never pay attention to them. Also, phishing scams start off with promises of money in a business proposition or through deals that sound too good to be true. Most of these mails are badly written with pathetic grammar and wrong spellings. Though not a sure shot way to spot phishing but can be a handy marker at times. If you come across such badly written email, never respond to them. If you are in doubt of such a mail, make a call to the telephone number given to check the authenticity of the claim. If there's no number, don't even bother.

To your credit

Credit cards are major sources of cybercrime and can be easily tampered with, if you are not careful enough with it. A stolen credit card can mean

the end of the world. So, it is important that you treat your credit card as carefully as cash.



Keep your card details, like the card number and CVV confidential.

If you get a new credit card, immediately sign at the back with permanent ink. If you still have old credit cards that have expired, cut them up to reduce the possibility of a misuse.

While swiping your card at stores, wait till the transaction has been completed. Check if the card returned to you was the one you had given and has not been tampered with in any way. This may seem like inconsequential but most cybercrimes are a result of negligence on the part of the user. So when you get the charge slip, total the amount to make sure that you are

not paying extra. Only then, sign it. Never leave blank spaces as it offers criminals a leeway to tamper with your card. On the same note, keep your purchase receipts just so that you can cross-check with your credit card statement. Vigilance can help you save trouble.

In case of transactions which you are sure that you have not made, contact your credit card service provider immediately. Pore over your statement every month to be clear. Ensure that your credit card statements are neatly filed and kept accessible at a single location. Your credit card statements contain sensitive information and have to be safeguarded. If you are closing your credit card, never throw away the statements. Shred them carefully so that it cannot be misused.

In case you are traveling abroad, inform your credit card service provider. Similarly, keep your company informed of any change of address so that your statements reach your new address safely. This way, such sensitive information won't get into the wrong hands.

Safeguard your credit

If you lose your credit card, inform your service provider immediately. Keep your toll free card number handy so that you can proceed with cancellation without delay. This would ensure that your stolen card is now swiped for large amounts.

Never allow anybody else to use your credit card. It is only yours and no matter how trusted the person in question is, never give away your card.

Keep your Personal Identification Number (PIN) a secret and never write it down. Also, never give out any information about your credit card, especially to those who are trying to sell you products through the phone. There are too many such false offers.

Never ever sign a blank cheque slip or leave space below your signature. Draw a line below the total amount and destroy any cancelled receipts at the earliest. Also, ensure that expired cards are not lying around. If it goes into the wrong hands, you might find yourself in a very large debt.

When shopping online, create a virtual credit card number that can be used only for one time. This way, you reduce the chance of exposing yourself to such fraudulent attempts. Keep your credit card with you at all times. Ensure that nobody knows where you keep it or what your PIN details are. Leaving such vital information lying around or carelessly handling your credit card can be a temptation for the other person, who could use your card for their personal use.

Before you ever give out information about your card to another company, insist on a complete set of references and information about the company and the product before actually revealing your details.

If you receive unsolicited calls from people claiming to be your credit card service provider and request for your account number, never give it. If the caller is indeed from your service provider, they would already know your details. In case of a doubt, ask the caller to notate on your file and call back on the number given at the back of your credit card and cross-check.

What's in a name?

While in Shakespearean era this would just be another argument, in our existence, your identity is as important as your bank details. Once stolen, your well-being can be seriously compromised. In 2008 alone, there were 10 million cases of identity theft worldwide in the US. More people are now adept at identifying attempts at identity theft. However, prevention still remains the best solution and you can do that by following the solutions given below.

Choose a strong password for your details. This should be so strong that people should not be able to guess it. You can use a simple cipher like the Vignere Cipher for this purpose. The internet will offer randomly generated passwords that can be unbreakable. Never use phone numbers or your vehicle numbers. And, add a capital letter to add strength to your passwords.

Be wary of people at the ATM or the supermarket, especially the types that look over your shoulder. While appearing uninterested or innocent, they might be sneakily observing your PIN details or your account balance. Ensure that you cover the monitor with your hand before keying in the important information. Even when there is nobody around, follow this practice as most people use binoculars or cameras to capture this data from far away.

Old billing statements and other documents should never be thrown in the dustbin. Instead, shred it carefully as there are people who would go through the dustbins in search of such incriminating information. Investing in a cross cut paper shredder that will completely destroy any piece of paper is actually a good idea. Ensure that the shredder doesn't just create strips of paper that can easily be patched up together. Instead, use a device that does a thorough job and for an extra measure, dump one half of the bill in one garbage bag will disposing the rest in another one. This may sound overcautious but it's better to be safe than sorry.

Secure communication

Credit card offers are often the vehicle of cybercrimes. Though you don't apply for the credit cards, tossing them carelessly in the dustbin would only mean that the miscreant can use your identity to apply for a new card. Call your credit card number and opt out of receiving such offers, especially by mail.

We live in an era of supersonic communication. But that doesn't mean that you don't keep an eye on the post box. The mail is a place where millions of personal information is handled every day and is the commonest route to identity theft. Pay attention to your email, especially the billing statements. Ensure that these statements are on time or better; opt for a paper-less statement through your email id. This way, you don't just reduce the risk to cybercrime but also do your bit for the environment.

Your computer is the hub for cybercrime. Many identity thieves use complicated software to break into your computer and elicit sensitive data like your passwords. You may not notice anything wrong but that doesn't mean that you are safe. Most cybercriminals use spyware and other stealth mechanisms to steal your data. The only way you can fight this is by installing a strong firewall in your computer, one that will provide utmost protection without wearing out the user experience.

When you are planning to get rid of your computer, ensure that you have erased all the information stored. Restore it to factory settings, for an added measure.

Most of us carry immense identifying information with us, either in our wallets or bags. If such should get stolen, it is easy for people to misuse the information to their advantage. Never carry credit cards or any other cards which can be used as a credit card. By doing this, you will reduce the damage, in case of theft. Carry if you must, ensure that you carry only one credit card. And, write SEE ID next to your signature.

Never carry any extra documents that you are not planning to use. Unless you are traveling, leave those extra checks and passport back home.

Social media safety

While using public computers, never check the "Save Password" box. Many social media forums auto check this box – so keep your eyes peeled for such possibilities.

Signing up for social media could be done with your full name. This way, you can prevent others from impersonating you on the internet. For those

who have common names and cannot go with a normal one, place some symbols between your first and last names. This may help differentiate you from others.

Ensure that your privacy settings are top notch. By doing this, you have the control of all the information that is being posted on your profile. Approve friend requests, links and tags beforehand and be careful of whom you choose to add as friend. Delete friends who you no longer keep in touch with.

It usually is a good practice to type in the name of the social networking site. Or, add a bookmark in your browser. The new scams on social media are done by emails that are similar to that of the social media provider. When you get such mails, assume the opposite – that it is a hoax.

Social media is a double edged sword and has to be used carefully. Never give out your travel plans on social media forums. This is the point where cybercriminals translate into real time threat, landing up at your home while you are not in town and burgling it. Never post about your whereabouts and especially, your residential address.

Most applications now have sign in options with social media. Never do that. This is just a great way to get access to your personal information on your profile. Else, read the terms and conditions carefully before you sign up. Otherwise, you don't know where your sensitive information may end up. Sadly, most company sell such databases of contact to businesses or private institutions, who are more often than not, up to no good. Exercise caution while you use the social networking sites. Not being cautious can mean that even your friends may lose their personal information in a bid to retrieve yours.

Your online reputation matters

Use extreme caution when opening links on social media sites. Even your friends can have their identities stolen on social media sites and post links that lead thieves to retrieve your personal information or hack your computer.

If you have children, lay down the ground rules of social media with them. Though youngsters may be more capable of making the most of social media, they might not understand its widespread ramifications, until it's too late.

Manage your online reputation. Start off with setting up a Google Alert for your name and also for those of your family. You can do this with your Gmail account, by clicking on the “More” tab on the Google toolbar. This option searches for your name on the internet and keeps you updated when any information with your name in it is used on the internet.

There are other such programs to help you stay on top of things. Sign up for a service that manages your online reputation and presence much better than Google. Steprep.com can be a good idea. Such services help you spot social media identity problems much ahead of time, if you use this regularly.

You can augment your internet presence by participating in online forums, blogs and social media. This way, you can ensure that nobody else uses your account. As much as possible, portray a positive personality online while shying away from anything religious, political or merely offensive.

Most hackers use “Forgot your Password” link to break open your account. Ensure that your security questions are not the ones that can be easily guessed, like your mother’s maiden name or your birthday. Make up your own questions or answers do that your personal information stays secure.

If you think that your social media account has been act, report immediately. Also, warn your friends over the phone or in person, so that they don’t get sucked into this vicious circle.

Regulate online transactions

E-commerce has grown by leaps and bounds and the result is that we shop more online than in real time. And let’s admit it. Online shopping is convenient and also saves time and effort. But if you don’t pay attention, your credit card details maybe misused, especially through online transactions.



Never buy from sites which you don't trust. Before giving out your password, check if the site is genuine. This way, you can ensure that you are on a site that is secure and respects your patronage.

While making online transactions, ensure that you are on a secure connection. Always check for the <https://> link and the symbol of the lock. If you don't find it, look out for other places to shop from, preferably one that allows for a secure transaction.

Online shopping should mostly be done on a personal computer. Public computers are meant for use by many members and this is not exactly the right place to share your credit information. These public systems save usernames, passwords and even cookies, making it easier to access information. So, use your personal computer.

Your password should be a high security one where you get alerts each time you make an online transaction. This is highly recommended for those who use a debit card. Most banks offer this service automatically but if yours doesn't, sign up for it right away. You can also opt for a 3D secure code which will offer additional protection. This is very helpful if you are a regular online shopper.

Use virtual keyboard to key in your important details. Most physical keyboards can be broken with key logger software. But the virtual keyboard is highly secure and safe from such attacks.

Use a VCC or a virtual credit card. This is handy as you can shop online without sharing much of your credit card information on the merchant website. This is a one-time usable credit card with a limited balance. This feature is usually available with your netbanking option. And ensure that you don't buy a VCC from any online dealer. When in doubt, approach your bank.

Finally, keep a track of your transactions as well as your account statement, which will show where you have purchased and when. In case of any unrecognised transaction, inform your bank immediately and lodge a complaint.

Beat that bully

The cyber bully is on the rise. Any type of bullying falls under the dominion of unpleasant and the cyber forum doesn't make it any different. Cyber bullying includes stalking, sending messages of a threatening nature, altering images and distributing them on the internet with the intentions of harassing or intimidating people.

Don't respond to nasty messages. With the mobile phones and social networking sites ruling our lives, some immature individuals post nasty comments, send berating SMS messages and share humiliating pictures of videos.

Before you post something on the internet, pause for a minute and think over the contents. While sharing anything personal, be very conscious. Even if you know most of the people on your friend list personally, the information can be misused. It could be copied and made public, and once it's on the internet, it's very difficult to remove it later on.

It pays to be courteous online. Manners never hurt anyone and this is the same in the online forum. This starts by treating people like the way you would like to be treated. Being mean can only attract troubles and bigger bullies picking on you.

In case you come across unflattering statements or statements on the internet that makes you uncomfortable, just ignore it or better, block the sender from your list. Most bullies are encouraged by retaliation and the situation would only get worse thereon.


If you are being subjected to unwanted, abusive message, report this to an adult who you trust – your parents or a teacher. They would inform the service provider of the email or phone service and the bully can be taken to task. This will mean that the person who you confide in should take a broader perspective and take action immediately. If things still continue, inform the cybercrime division in your city. They would immediately get working on the culprit.

Before you approach the authorities, ensure that you have enough evidence. Save the messages or conversation thread on your social networking site. Again, get your parents or another adult into the picture. If this gets serious, approach the police.

If you see another person fall a victim to this behaviour, don't just watch. Encourage your friend or the person bullied to take action. Stand up for the victim. You can enlist your parent's help or even discuss this with your teacher. They would be able to take a call on this and safeguard you in case the issue turns vicious.

In conclusion

While the internet is a wonderful device and has become an imperceptible part of our lives, there's a lot out there that could cause serious trouble. The flip side is cybercrime and sadly, it is on the rise. The best thing to do is to

be prepared. Follow these simple rules. Use your common sense and act smart. Think before you act and while conducting any online transactions, keep a wary eye. Being aware can help you stay away from cybercrime. After all, the internet can be full of good experiences if you take preventive measures and keep cyber criminals at bay with your resourcefulness. 

[illegible]

[illegible]

[illegible]



All this and more in the
world of Technology

**VISIT
NOW**



www.thinkdigit.com

Join 70000+ members of the Digit community



<http://www.facebook.com/thinkdigit>

facebook

digit magazine

Digit magazine [Like](#)

Your favourite magazine on your social network. Interact with thousands of fellow Digit readers.

- Wall
- Info
- Jobs
- Photos
- Videos
- Events
- Notes

<http://www.facebook.com/IThinkGadgets>

facebook

I Think Gadgets Corporate/Institution [Like](#)

An active community for those of you who love mobiles, laptops, cameras and other gadgets. Learn and share more on technology.

- Wall
- Info
- Jobs
- Photos
- Videos
- Events
- Notes

<http://www.facebook.com/GladtoBeAProgrammer>

facebook

Glad to be a Programmer Community [Like](#)

If you enjoy writing code, this community is for you. Be a part and find your way through development.

- Wall
- Info
- Jobs
- Photos
- Videos
- Events
- Notes

<http://www.facebook.com/devworx.in>

facebook

devworx Community [Like](#)

devworx, a niche community for software developers in India, is supported by 9.9 Media, publishers of Digit

- Wall
- Info
- Jobs
- Photos
- Videos
- Events
- Notes